Exploring Trusted Access

Beginning the journey toward a more secure modern workplace

Henrik Nitsche

Security Sales Manager
|DACH-CEE

Erleben,
was verbindet.

Manage and Secure
Apple at Work

71,000+ Active Jamf Customers	**30M+** Devices Running Jamf	**100k+** Jamf Nation Members
7 of the top **10** Top technology companies as ranked by Fortune [1]	**9** of the top **10** Largest companies as ranked by Fortune [1]	**22** of the top **25** Valuable brands as ranked by Fortune [2]

jamf

Erleben, was verbindet.

1. As ranked by Fortune as of 6/30/2022. 2. As ranked by Forbes Most Valuable Brands list as of 6/30/2022.

Device Management

Identity & Access

Endpoint Security

jamf

Erleben, was verbindet.

only **Authorized Users**

on **Enrolled Devices**

that are **Secure & Compliant**

can **Access Sensitive Data**

Trusted Access

jamf

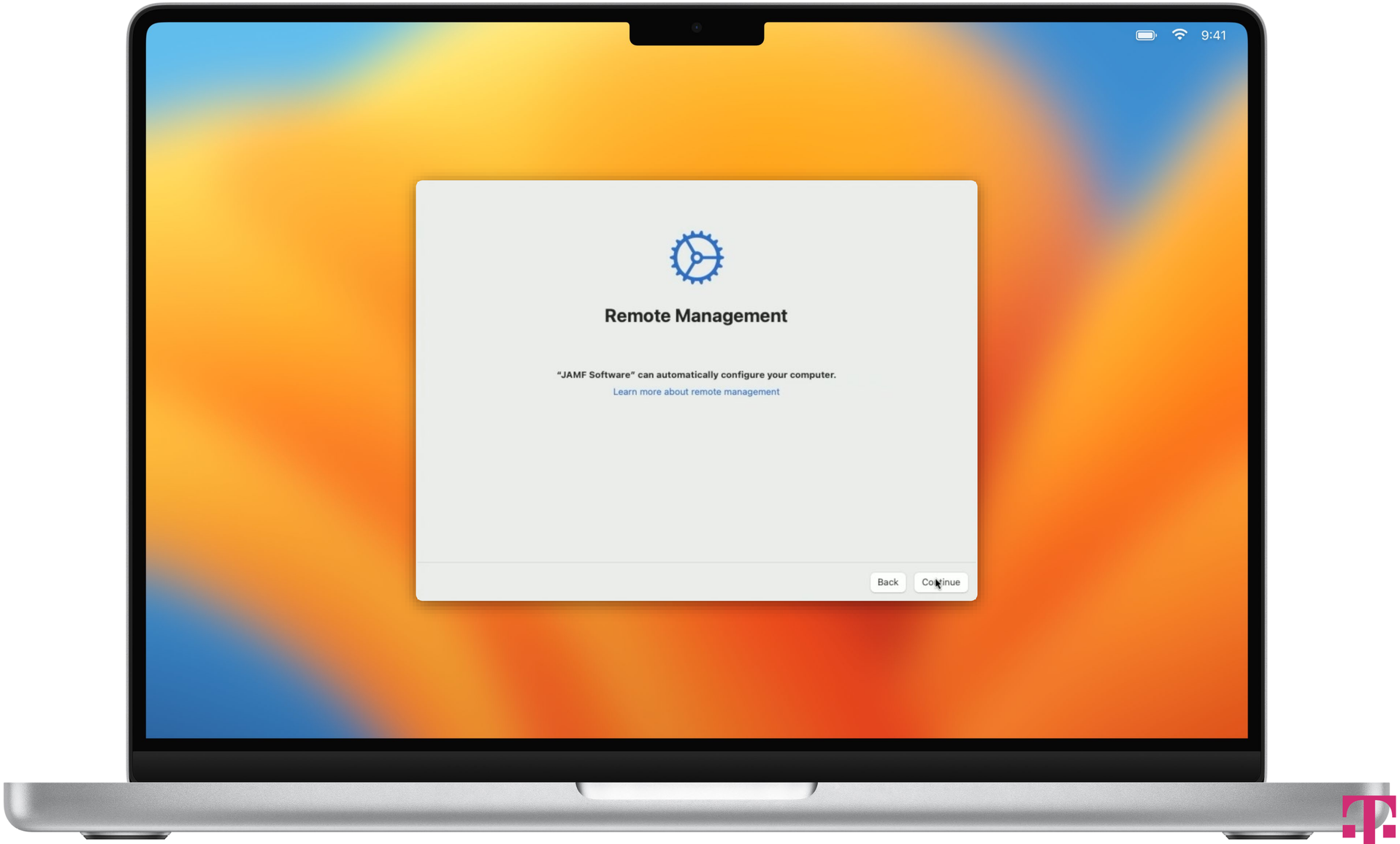
Erleben,
was verbindet.

Achieving **Trusted Access** with Jamf

Erleben,
was verbindet.

jamf

Enrolled Devices

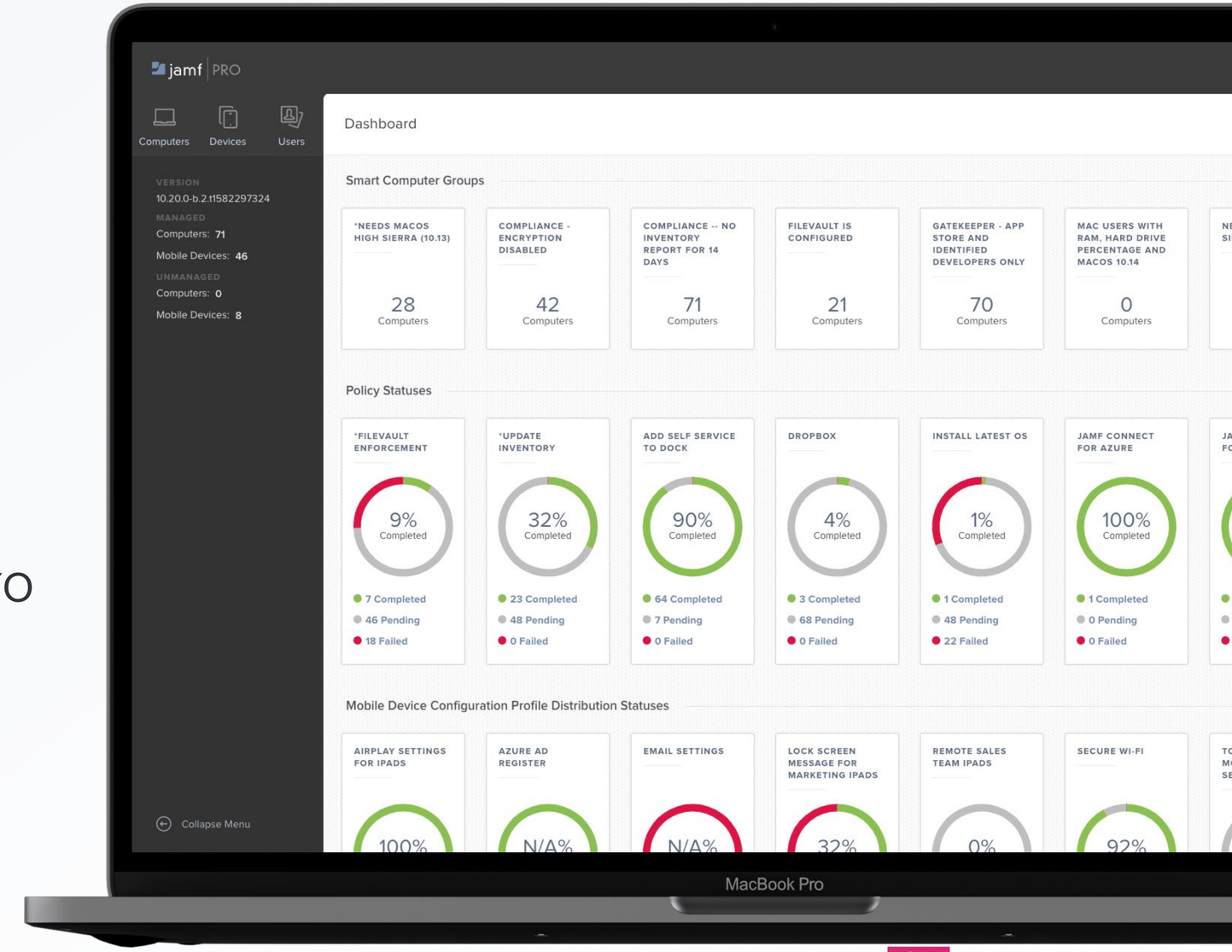


jamf

macOS iOS iPadOS

Erleben, was verbindet.

Establish device trust
Jamf Pro



Management is a key workflow component

- Provides critical configs that enable productivity
- Provides visibility into basic device risk
- Provides threat remediation options
- Can be achieved on both company-owned & BYO

jamf

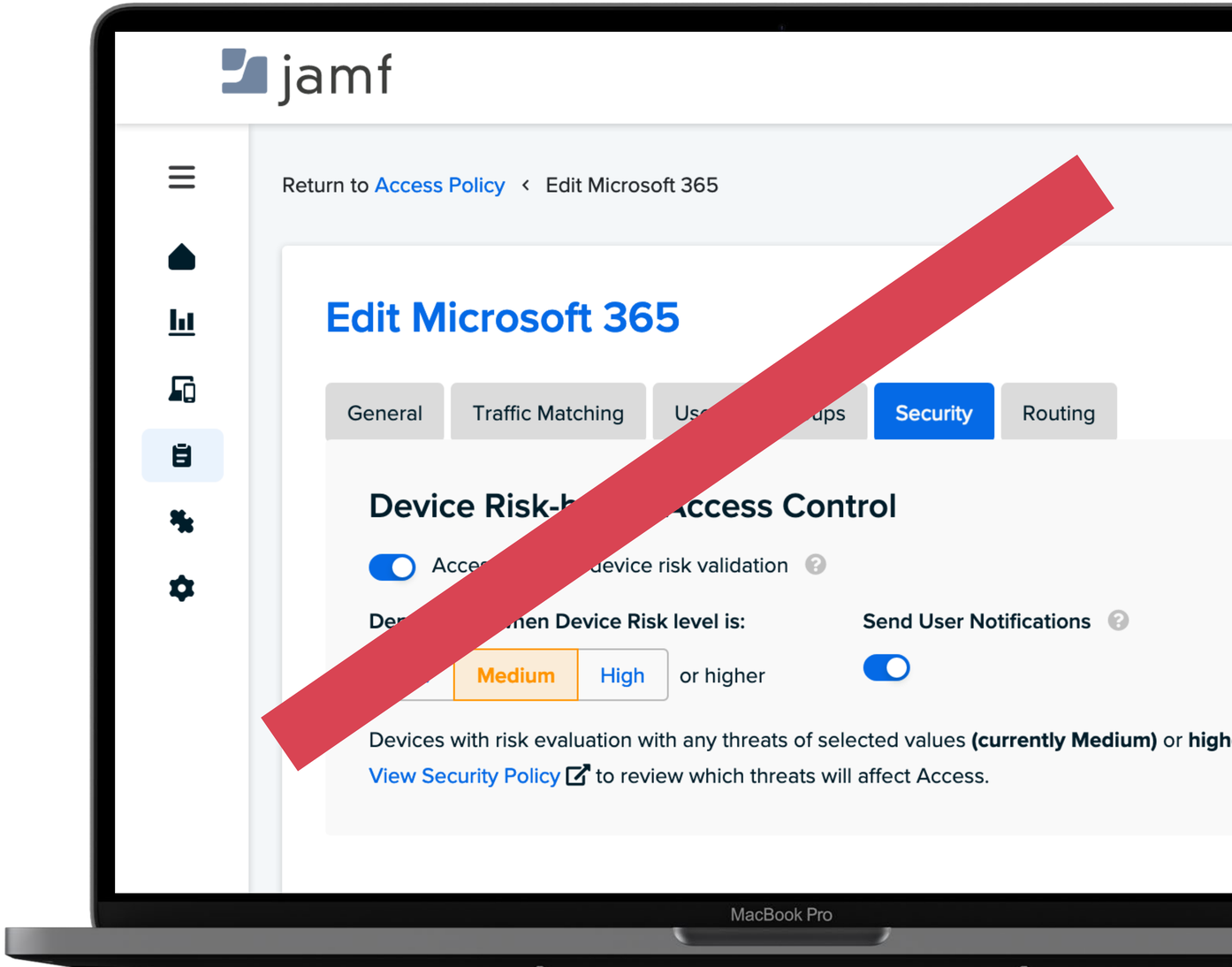
Erleben, was verbindet.

Establish device trust

Enrolment as baseline risk assessment

Enrolment status signaling to influence access

- Enrolment assessment as baseline ‘risk’ check
- Automates enforcement of enrolment requirement
- Can support integrations with 3rd party UEMs

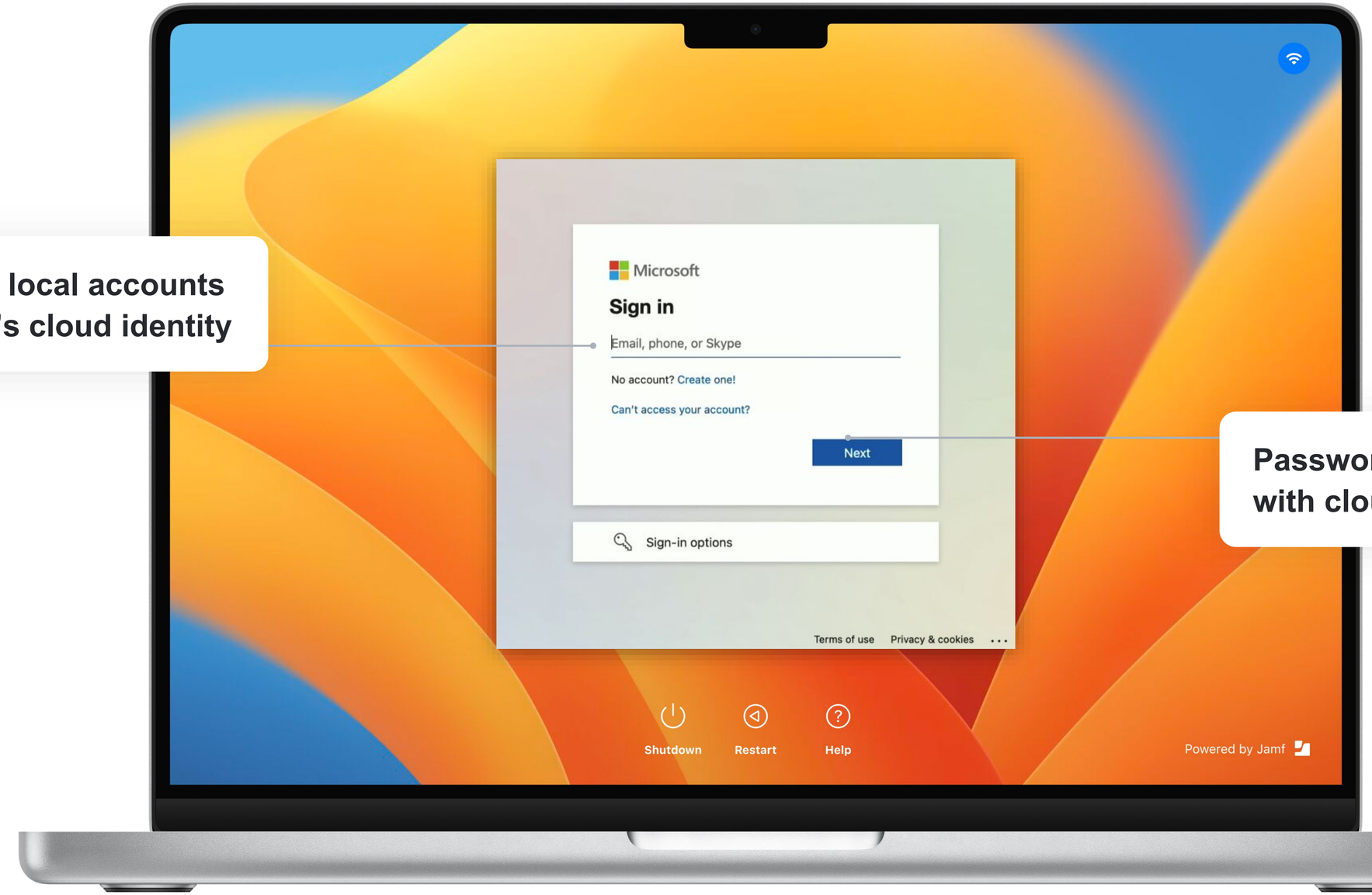


jamf

Erleben,
was verbindet.

Verified Identities

Provision local accounts with user's cloud identity



Password stays in sync with cloud identity

jamf

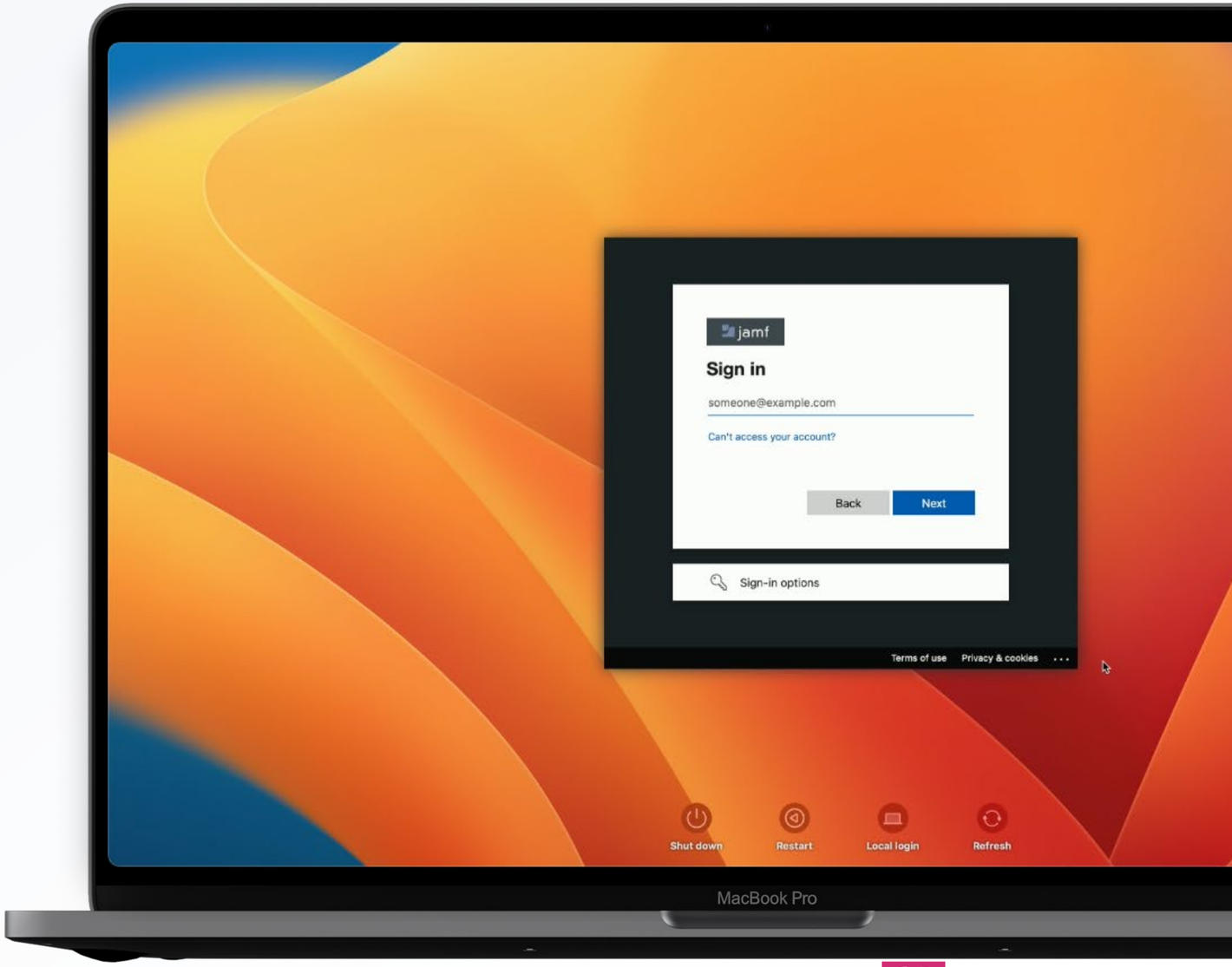
macOS

Erleben, was verbindet.

A truly **zero-touch experience**

From a seamless onboarding experience to empowering users with cloud-based identity on Mac and providing access to cloud or on-premise resources, the overal device experience is an important factor in a user's journey and benefits their productivity.

- Streamline user login with cloud-based identity
- Enforce multi-factor authentication with every login
- Eliminate password-related tickets with password synchronisation
- Provide secure access to resources hosted in the cloud or on-premises



jamf

Erleben,
was verbindet.

Protected Endpoints

Audit device security benchmarks

Automatically block and quarantine malware

jamf

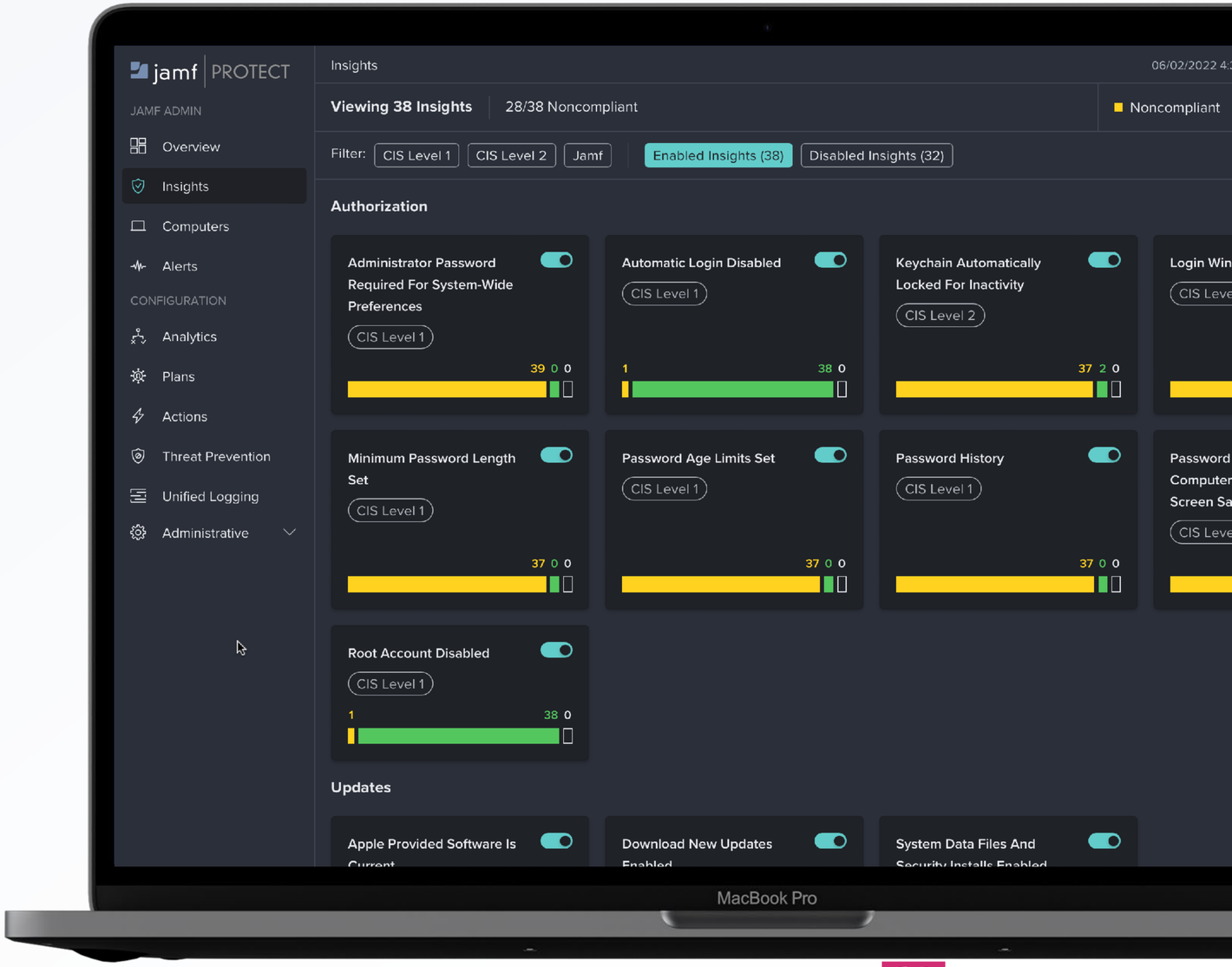
macOS iOS iPadOS

Erleben, was verbindet.

Compliance Management

Establish and Maintain Secure Baselines

- **Establish secure device baselines**
  Audit devices against “known good” standards
- **Manage mobile configuration vulnerability**
  Monitor for adherence to organizational standards
- **Maintain secure standards over time**
  Broad remediation options to address risk
- **Purpose-built security for Apple**
  Same-day support, native frameworks, great experience



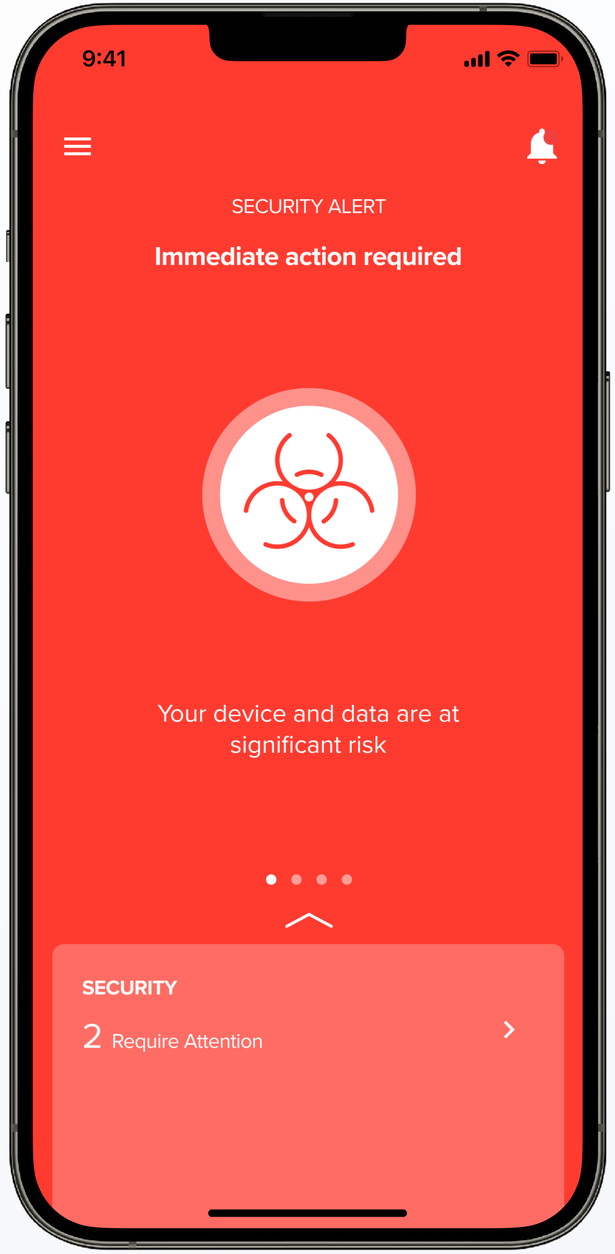
jamf

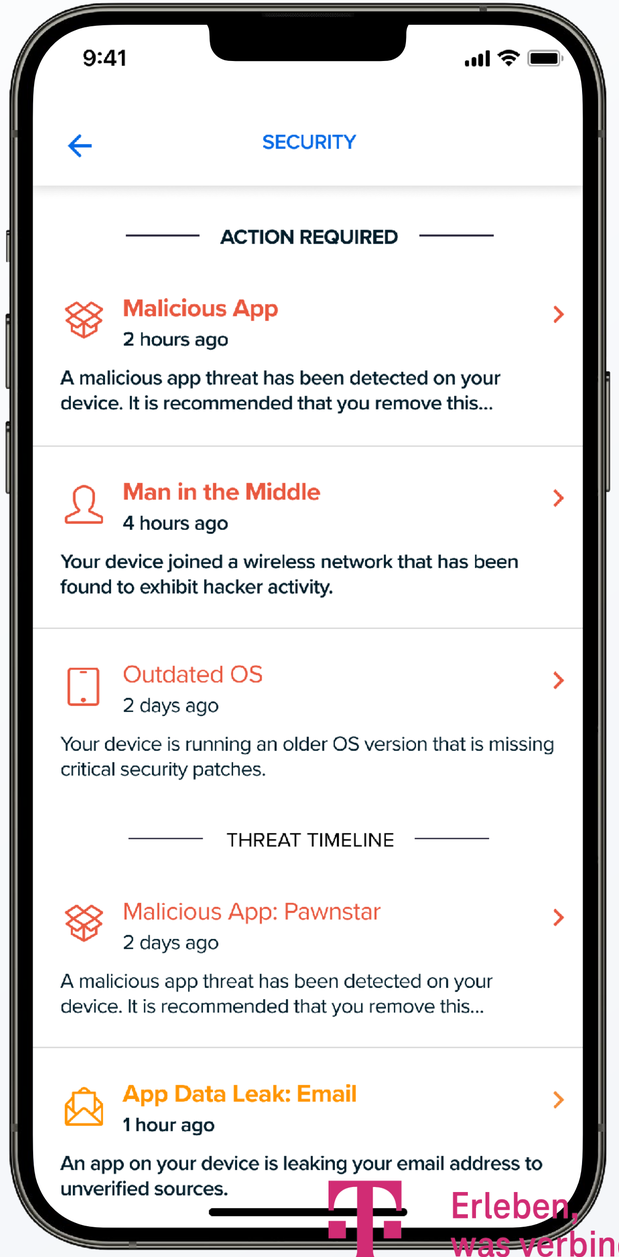
Erleben, was verbindet.

Mobile protection with **Jamf Protect**

- Protect iOS, iPadOS and Android devices
- Prevent cyber threats like phishing
- Users can view alerts and security timeline

iOS iPadOS android Windows





jamf

Erleben, was verbindet.

GOV.UK

Home > Government

News story

TikTok banned on UK government devices as part of wider app review

Social media app TikTok has been banned on government electronic devices, the Cabinet Office has announced today.

From: Cabinet Office and The Rt Hon Oliver Dowden CBE MP
Published 16 March 2023

La Liga fined over app that spied on illegal match screenings

- **€250,000 fine imposed by data watchdog**
- **'We profoundly disagree with this decision'**

Barcelona celebrate in April after winning the 2018-19 La Liga title. An attempt to protect the TV rights from pirated use has led to a fine. Photograph: Manu Fernández/AP

La Liga has been ordered to pay a €250,000 (£220,000) fine after Spain's data protection watchdog said its official match-following app had been used to spy on bars that had been showing games illegally.

APPLE / TECH / POLICY

Apple is reportedly preparing to allow third-party app stores on the iPhone

/ Bloomberg's Mark Gurman reports Apple will respond to upcoming EU rules with next year's iOS 17 update. But it could still have strings attached, like only being available in Europe or only allowing installation of approved apps

Jamf Threat Labs

Leading Edge of Apple Threat Research

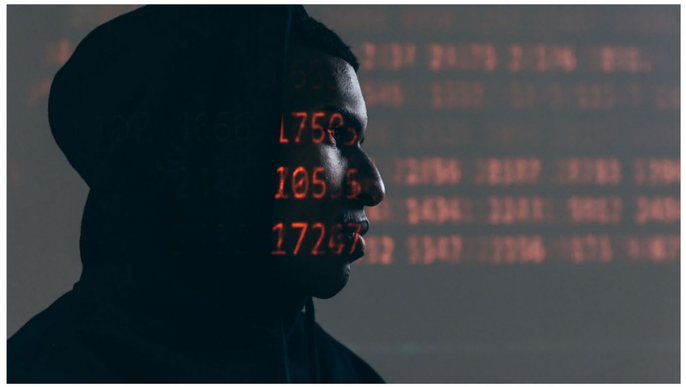
Jamf Blog

April 17, 2023 by Jamf Threat Labs

Threat advisory: Mobile spyware continues to evolve

Jamf Threat Labs

Jamf Threat Labs examines two sophisticated spyware attacks and provides recommendations for organizations to defend users from increasingly complex threats.



Erleben,
was verbindet.

Jamf Threat Labs

Leading Edge of Apple Threat Research

Experienced threat researchers, cybersecurity experts, and data scientists with skills that span penetration testing, network monitoring, malware research, and app risk assessment primarily focused on Apple and mobile ecosystems.

- Industry-leading platform expertise and threat intelligence
- Elegant implementation for lightweight user experience
- Unparalleled adoption and support of the Apple ecosystem

20+ **Years Experience**

securing the Apple ecosystem

Pegasus

discoveries of iOS spyware including Pegasus

Mac Zero-Day

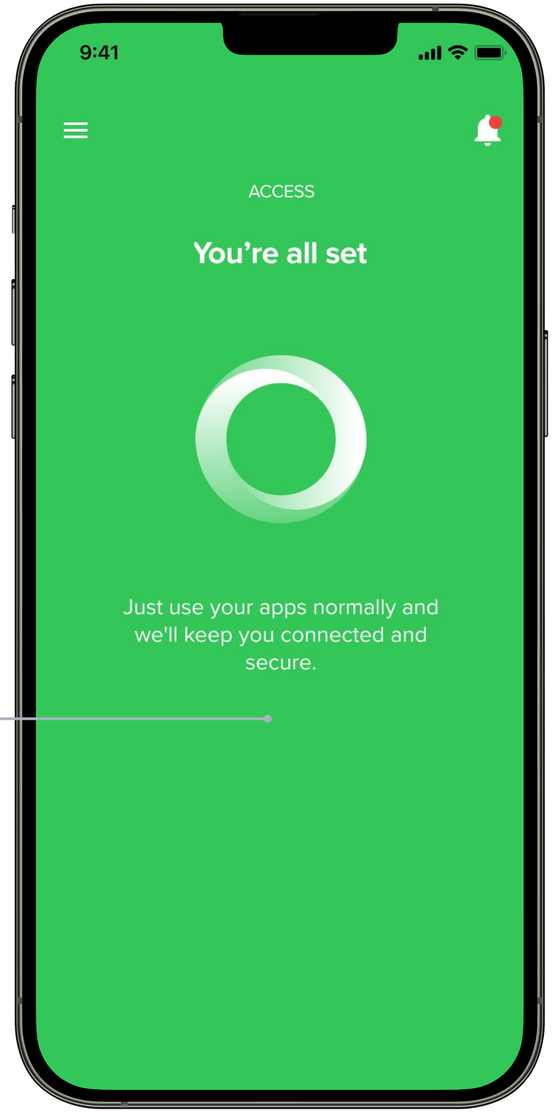
vulnerability exploitation discoveries

Erleben, was verbindet.

jamf

Erleben,
was verbindet.

Zero Trust Access



Continuous device security monitoring

Seamless experience

jamf

macOS iOS iPadOS android Windows

Erleben, was verbindet.

Restrict access to Trusted IPs only

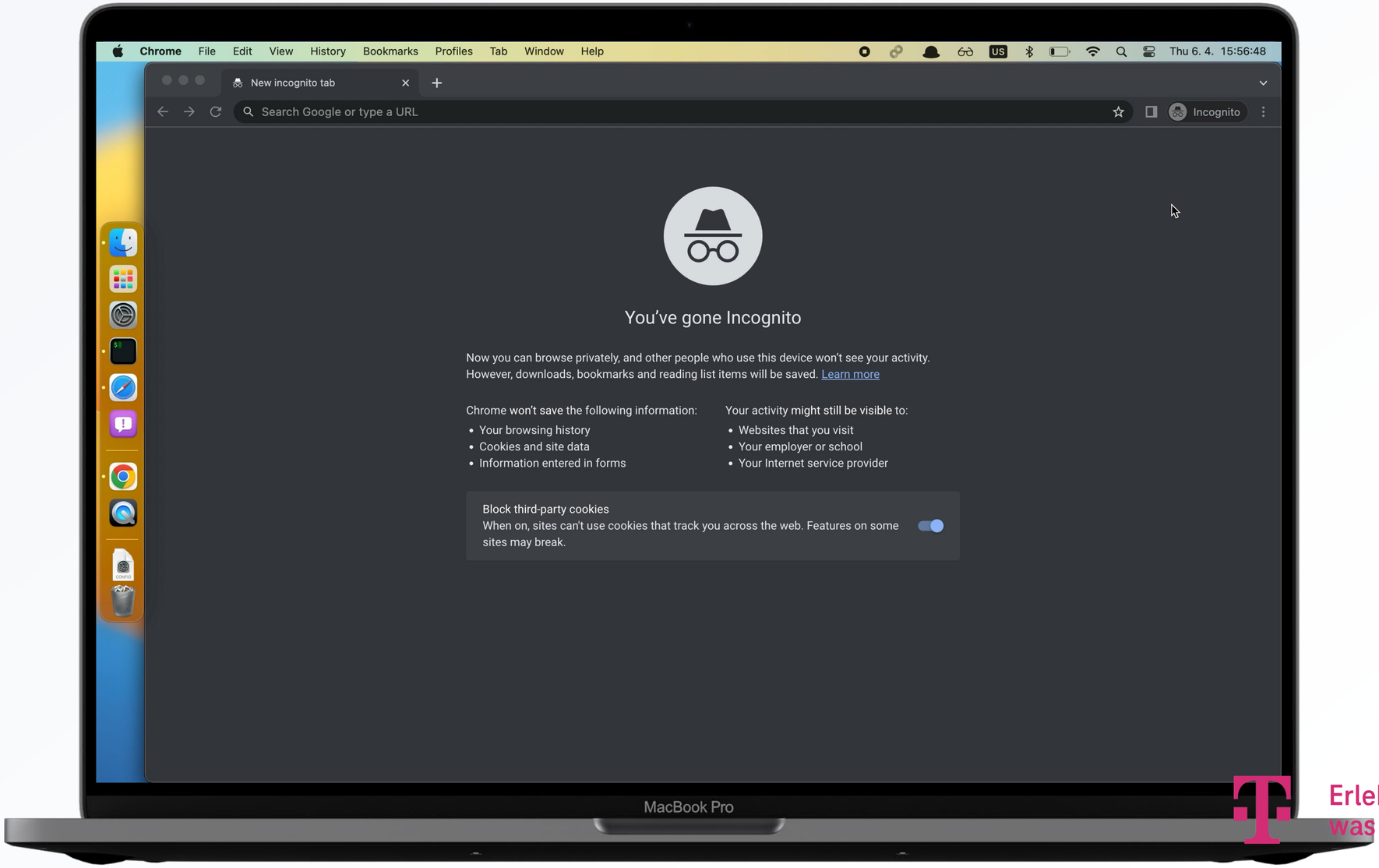
Jamf Trust is being enabled and device posture is being checked prior enablement

Access denied as we are not connecting from a Trusted IP

jamf

Erleben, was verbindet.

Continuous Conditional Access



jamf

Erleben, was verbindet.

Automation & Remediation

Suspend Conditional Access Enforce Disk Encryption Lost Mode **Kill Process**

Erase Device **Suspend App Access** Execute Script **Update OS** Collect Logs

Erase Work Data from BYOD Enforce Passcode Initiate Remote Access **Restrict App**

Reset Local Account Disable Hotspot **Shut Down Device** Disable Bluetooth

Reset Passcode **Update App** Restrict WiFi Network **Lock Device** Restart Device

Manage Activation Lock **Remove App** Manage Firmware Password **Notify User**

jamf

Erleben,
was verbindet.

Device Management

Identity & Access

Endpoint Security

jamf

Erleben, was verbindet.