All You Need To Know If You’ve Been Binding Macs

Sean Rabbitt

Sr. Consulting Engineer, Identity and Access Management
Jamf

All You Need To Know If You’ve Been Binding Macs

Agenda

Jamf Intro

Macs & Binding

CVE-2021-42287

Speculation To The Future

Unbinding & Best Practices for Mac

Leveraging Jamf tools for success

Next Steps

jamf

Helping organizations succeed with Apple

Macs & Binding

What did on-prem AD get you?

Directory services

Group membership info

Central account management

Group policy… sort of on

Resource access management

It also gave you challenges…

Binding to Active Directory

Password Keychain Lockouts

Updating Users while Remote

Updating from existing set up

Keeping BYOD out of cloud

CVE-2021-42287

Recommendation:

Don’t Bind Macs

Bind Windows … to Azure.

CVE-2021-42287

Explain it like I’m five.

- Random user on Reddit

CVE-2021-42287

Spoof a domain controller

Authentication Authority Vulnerability

Privilege escalation on Macs

Patch breaks binding

Become domain admin in 60 seconds

References

Fortinet: https://www.fortinet.com/blog/threat-research/cve-2021-42278-cve-2021-42287-from-user-to-domain-admin-60-seconds

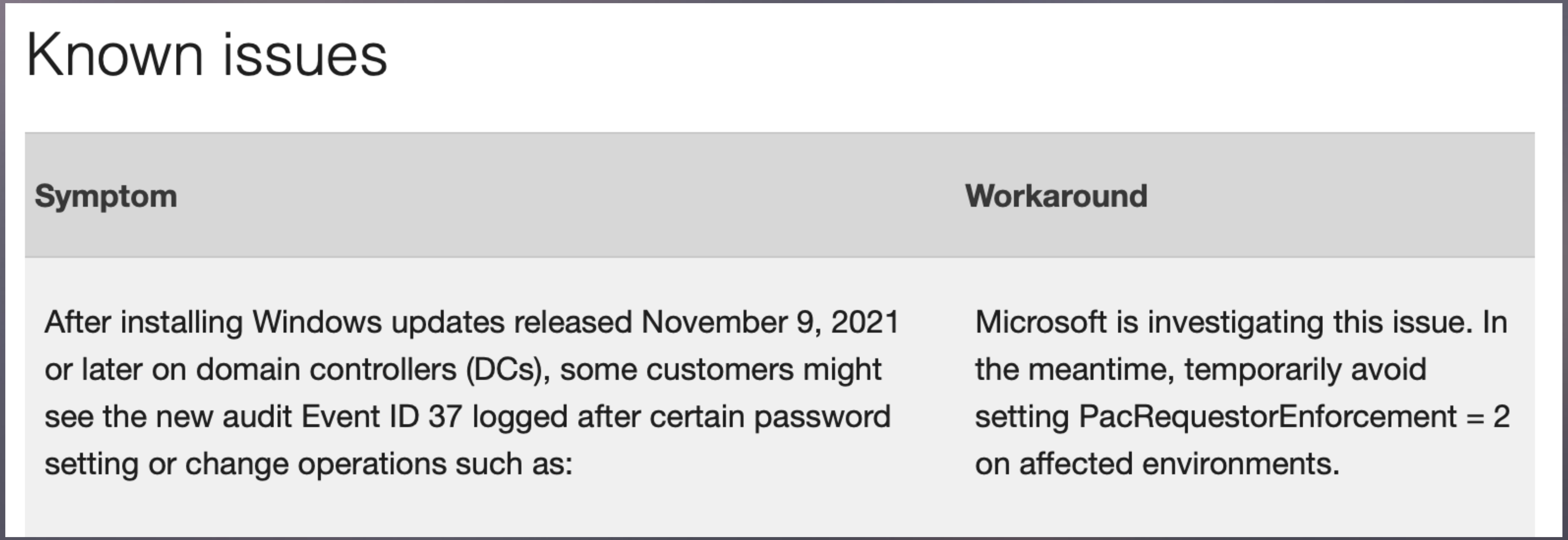
Microsoft: https://support.microsoft.com/en-us/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041

Jamf: https://www.jamf.com/blog/advisory-macos-ad-cve/

Jamf Nation: https://community.jamf.com/t5/jamf-pro/unable-to-add-server-authentication-server-failed-to-complete-the/m-p/255209

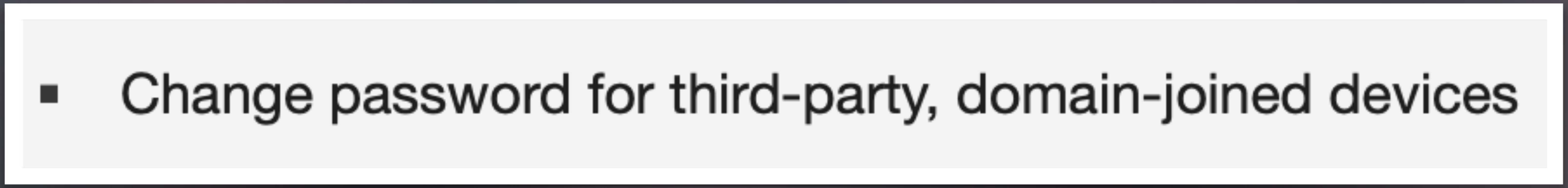
The Fix for CVE-2021-42287 Broke Mac Binding.

Update: 22 March 2022



Known issues

Symptom	Workaround
After installing Windows updates released November 9, 2021 or later on domain controllers (DCs), some customers might see the new audit Event ID 37 logged after certain password setting or change operations such as:	Microsoft is investigating this issue. In the meantime, temporarily avoid setting PacRequestorEnforcement = 2 on affected environments.



- Change password for third-party, domain-joined devices

https://support.microsoft.com/en-gb/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041

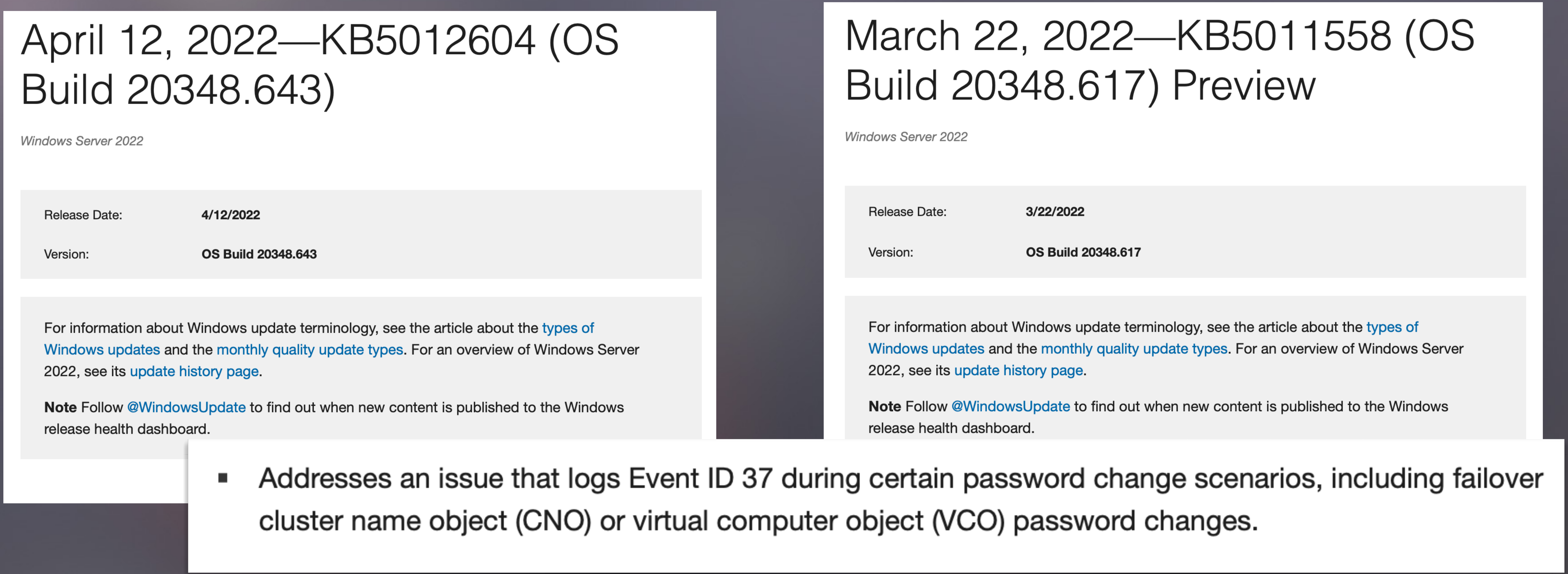
What is Enforcement Mode?

> “Starting with the July 12, 2022 Enforcement Phase update, Enforcement mode will be enabled on all Windows domain controllers and will be required.”

- KB5008380, Microsoft

BREAKING NEWS

12APR2022 - Server Hotfix



April 12, 2022—KB5012604 (OS Build 20348.643)

Windows Server 2022

Release Date:	**4/12/2022**
Version:	**OS Build 20348.643**

For information about Windows update terminology, see the article about the types of Windows updates and the monthly quality update types. For an overview of Windows Server 2022, see its update history page.

Note Follow @WindowsUpdate to find out when new content is published to the Windows release health dashboard.

March 22, 2022—KB5011558 (OS Build 20348.617) Preview

Windows Server 2022

Release Date:	**3/22/2022**
Version:	**OS Build 20348.617**

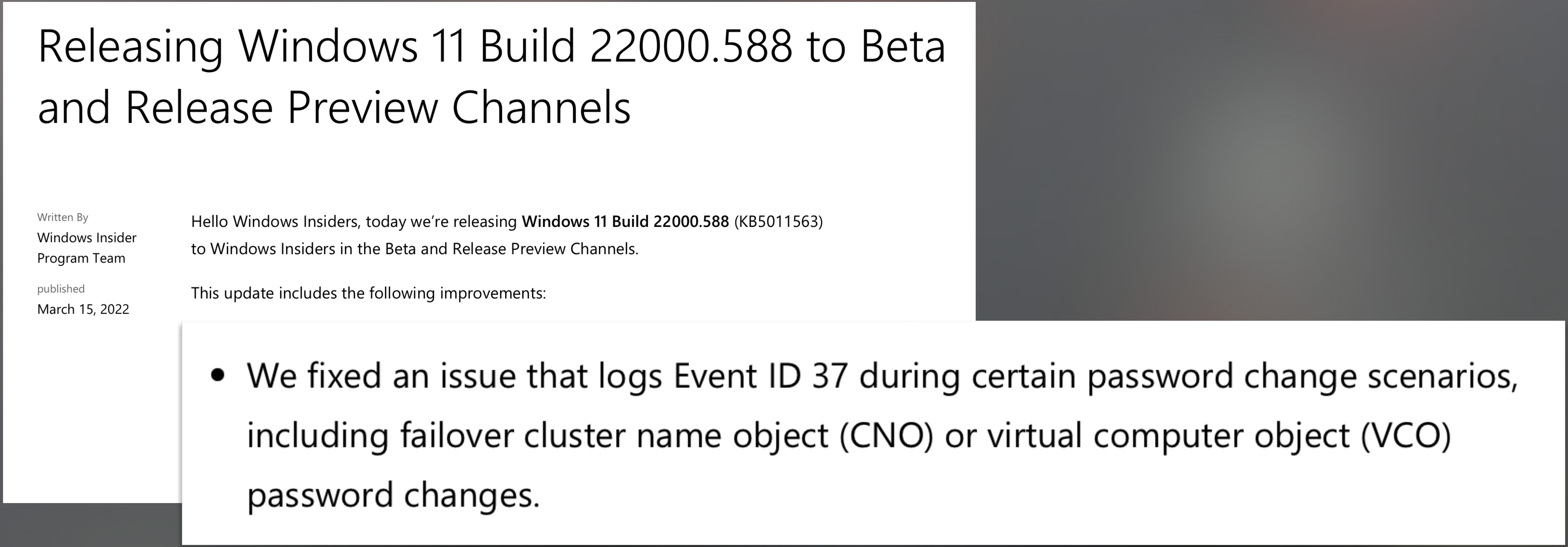
For information about Windows update terminology, see the article about the types of Windows updates and the monthly quality update types. For an overview of Windows Server 2022, see its update history page.

Note Follow @WindowsUpdate to find out when new content is published to the Windows release health dashboard.

- Addresses an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes.

https://support.microsoft.com/en-us/topic/april-12-2022-kb5012604-os-build-20348-643-25216e88-f9c1-4b9f-a131-8f8b1149d0bb

Client Hotfix Preview



Releasing Windows 11 Build 22000.588 to Beta and Release Preview Channels

Written By
Windows Insider Program Team

published
March 15, 2022

Hello Windows Insiders, today we're releasing **Windows 11 Build 22000.588** (KB5011563) to Windows Insiders in the Beta and Release Preview Channels.

This update includes the following improvements:

- We fixed an issue that logs Event ID 37 during certain password change scenarios, including failover cluster name object (CNO) or virtual computer object (VCO) password changes.

https://blogs.windows.com/windows-insider/2022/03/15/releasing-windows-11-build-22000-588-to-beta-and-release-preview-channels/

Speculation Time

History: OS X Lion

July 20, 2011:

“Authentication server encountered an error while attempting the requested operation”

October 12, 2011:

“Improve Active Directory and LDAP integration.”

Source: https://web.archive.org/web/20141123222818/http://support.apple.com/en-us/HT202262

What Will Break

Centralized identity management

Distribution of certificates

Management policies

FileVault and Keychain passwords

Unbinding - What’s Different

AD policy vs. MDM management

User-level Configuration Profiles

Certificates and Networks

User Management

Zero-trust via Identity Provider

AD Group Policy

Based on Windows administration

Issues translating Win to Mac

Certs based on binding

Mobile/Network accounts

AD password management

jamf

MDM Management

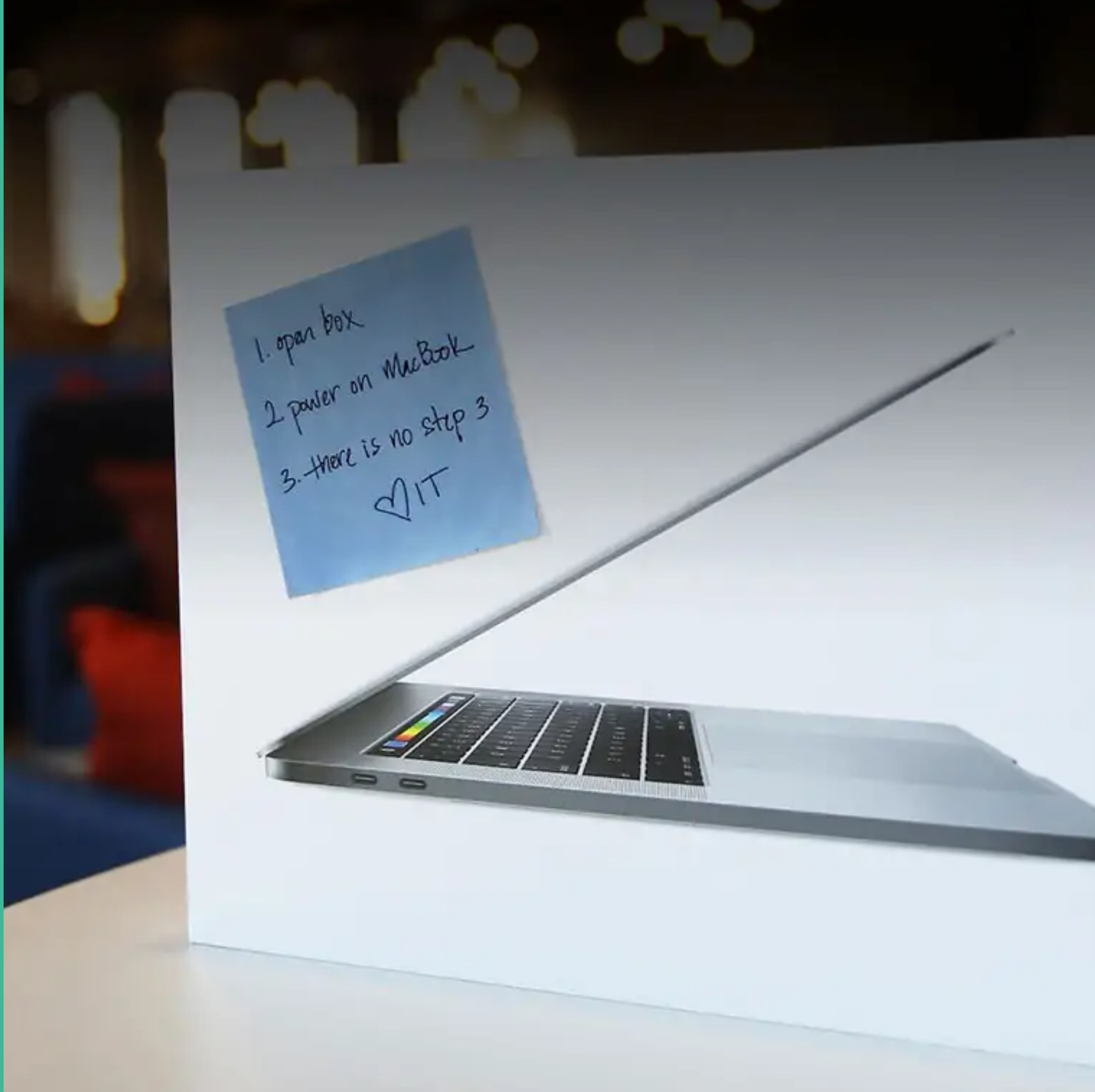
Native Apple commands

Multiple path to get certificates

Local user accounts

Reporting status of fleet

Active vs. passive management



User-Level Configuration

MDM-Managed Users

Machine Level Configuration

Images: Wikipedia

802.1x RADIUS Certificates

User level config profile certs ❌

Username / password ❌

Machine Based SCEP certs ✅

Networking and VPN tools

Cisco AnyConnect

Cisco ICE

Jamf Private Access

Jamf Threat Defense

User Management

Solution	Creates User Accounts	Password Sync	Gets Kerberos Tickets
Setup Assistant	First account only	❌	❌
Apple Kerberos SSO Extension	❌	✅	✅
NoMAD Login & NoMAD	✅	✅	✅
Jamf Connect	✅ Anywhere	✅ Anywhere	✅ On-Premises or VPN

Zero-Trust via IdP

https://help.okta.com/en/prod/Content/Topics/Mobile/Okta_Device_Trust_Jamf_macOS_Devices.htm

Trust user on device vs. trust device

Steps To Resolution

Steps To Resolution

- Unbind Macs or test patched AD servers before July 12, 2022
- Manage with MDM instead of AD Group Policy
- Manage users on device with Cloud Identity Providers
- Evaluate networking tools and access to organization resources
- Start planning for Zero Trust and Zero Touch Onboarding

Tools for Resolution

jamf | CONNECT

What is it?

Jamf Connect simplifies the provisioning process with Apple by allowing the user to authenticate against a cloud identity provider.

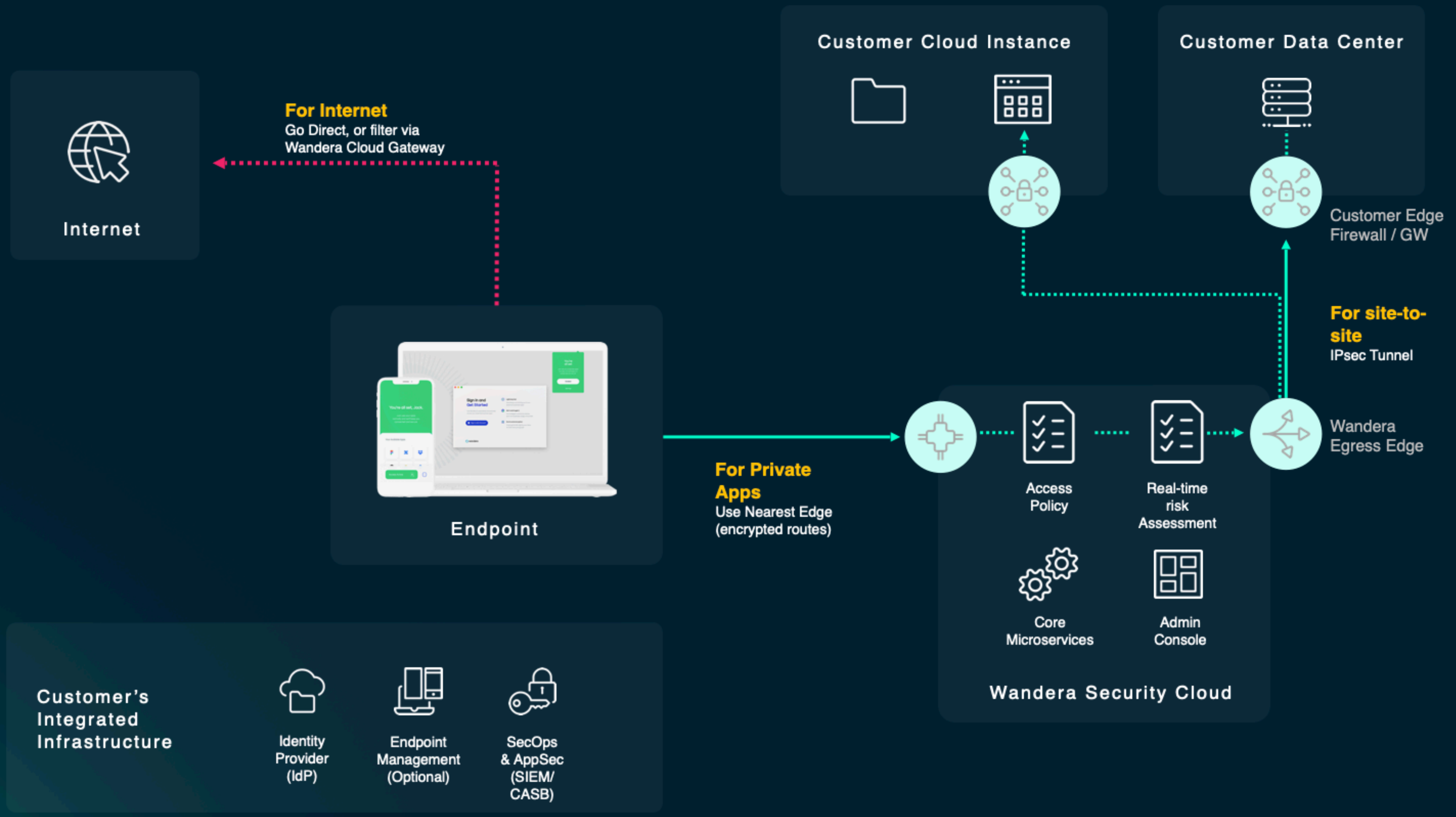
Jamf Connect

Provisioning

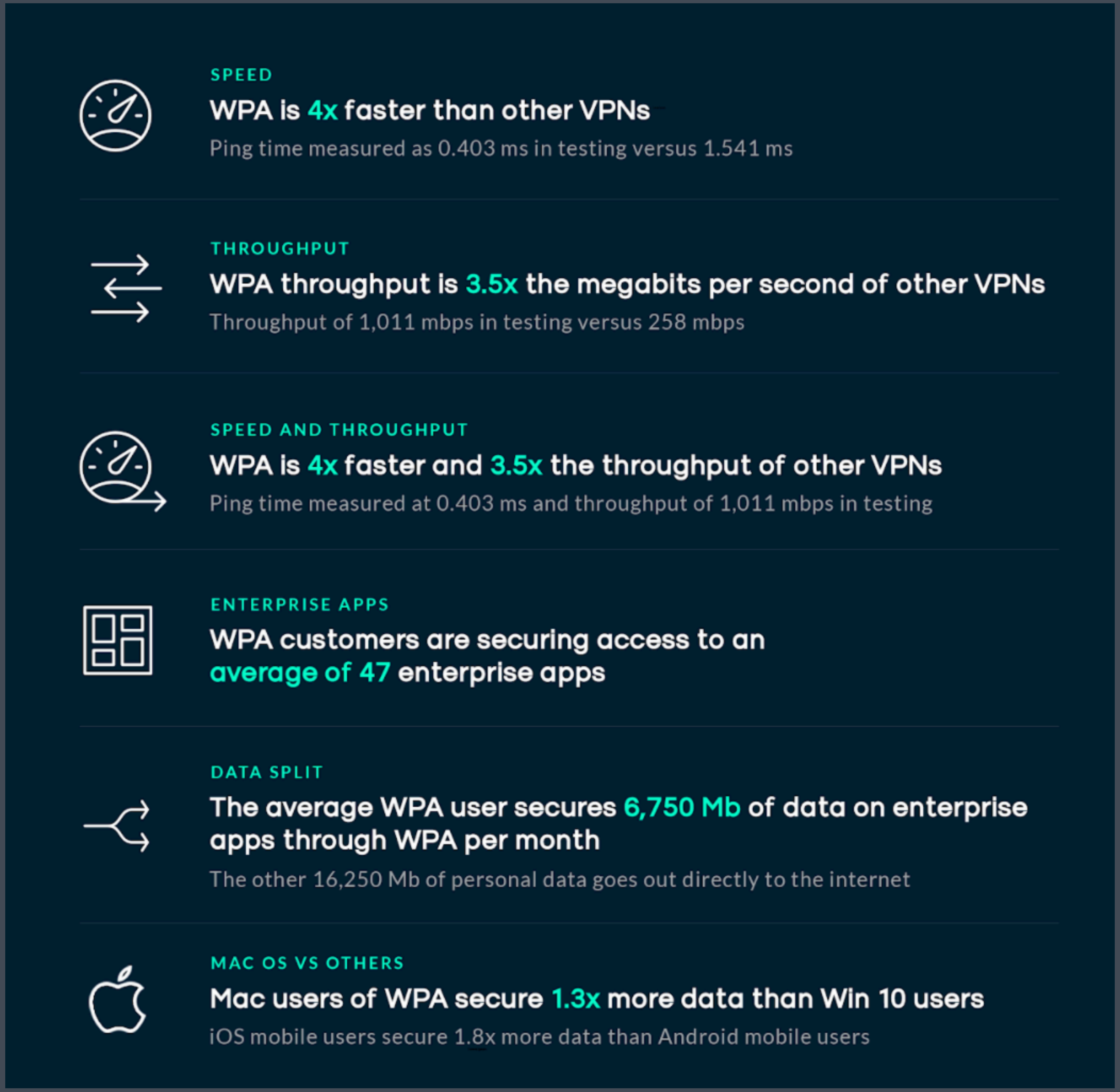
Identity Management

Password Sync

Private Access Client-initiated ZTNA architecture



Private Access



SPEED

WPA is 4x faster than other VPNs

Ping time measured as 0.403 ms in testing versus 1.541 ms

THROUGHPUT

WPA throughput is 3.5x the megabits per second of other VPNs

Throughput of 1,011 mbps in testing versus 258 mbps

SPEED AND THROUGHPUT

WPA is 4x faster and 3.5x the throughput of other VPNs

Ping time measured at 0.403 ms and throughput of 1,011 mbps in testing

ENTERPRISE APPS

WPA customers are securing access to an average of 47 enterprise apps

DATA SPLIT

The average WPA user secures 6,750 Mb of data on enterprise apps through WPA per month

The other 16,250 Mb of personal data goes out directly to the internet

MAC OS VS OTHERS

Mac users of WPA secure 1.3x more data than Win 10 users

iOS mobile users secure 1.8x more data than Android mobile users

jamf

Path to Success

Path to Success

- Avoid Binding
- Add device login with cloud IdP credentials
- Use Jamf Pro or similar MDM to manage
- Use Jamf Connect to sync local passwords
- Use Jamf Private Access to reach resources

Want to learn more?

- Request a demo or trial of Jamf Connect and Jamf Private Access
- Expertly guided proof of concept
- Have a consult on achieving zero-trust with Jamf
- Schedule a call with our team and any of our authorized partners
- Contact us: info@jamf.com

Thank you

Q & A