jamf

Jamf Blog <https://www.jamf.com/blog/>

September 19, 2023 by Haddayr Copley-Woods

JNUC 2023 Keynote

Jamf Nation User Conference <https://www.jamf.com/blog/category/jamf-nation-user-conference/>

JNUC 2023 got off to an announcement-packed start with our brand-new CEO John Strosahl. He and other members of the team, along with our partners, spoke about the growth of Apple, the introduction of Trusted Access and Jamf Pro 11— and how closely security and management must work in harmony to keep businesses and schools productive and secure.

John Strosahl, Jamf's CEO, kicked things off with a welcome to the excited crowd in Austin, as well as the thousands more joining remotely.

Austin was our biggest JNUC yet with more than 3,000 in-person and virtual attendees and over 150 sessions covering a wide array of topics.

“A lot has happened since we last got together," said Strosahl. "I'm pleased and humbled to lead Jamf as its new CEO and to continue partnering with Jamf Nation to understand your needs and help you all positively impact the employees, students and patients you serve.”

Strosahl outlined the uncertainty we all face in our work lives and the challenge to do more with less.

“We are facing a more dynamic threat landscape than ever before,” added Strosahl. “Toss in a growing remote workforce, and it’s fair to say we all have a lot on our plates.”

“But one thing hasn’t changed,” he said. “Our focus on helping organizations succeed with Apple hasn’t and won’t change, because we are needed now more than ever.”

Apple growth

Apple adoption is on the rise. More enterprises are turning to Mac. The International Data Corporation (IDC) anticipates a 20% jump in Mac <https://www.idc.com/getdoc.jsp?containerId=prUS51184723>computers <https://www.idc.com/getdoc.jsp?containerId=prUS51184723>sold to business users this year and next <https://www.idc.com/getdoc.jsp?containerId=prUS51184723>. iPhones are already the dominant provider in many geographies for employee devices, and iPads are being used in more industry workflows than any other device.

“When given a choice,” said Strosahl, “today’s workforce chooses Apple.”

It's because of that choice that we believe Apple will be the predominant endpoint in the enterprise.

Challenges of a platform-agnostic tech stack

The reality for many Jamf customers is that delivering a consumer-grade Apple experience in the workplace, school or medical facility is hard.

Some organizations try to stitch together different management and security solutions, which can lead to complex integration and will lead to a poor user experience.

“When you take a platform-agnostic approach to your tech stack,” said Strosahl, “you’re unable to support the rich array of experiences that are possible with Apple devices.”

Jamf AND

“We continue to offer and expand our industry-leading Apple management AND security solutions because customers have told us you need more from Jamf to make Apple successful in your organization,” said Strosahl.

Jamf helps our customers deliver an experience that their users love AND one that their organization trusts.

“And we relentlessly bridge the gap between what Apple provides AND what the enterprise needs,” said Strosahl, “everything we do and will do in the future is focused on that 'AND.'”

“At Jamf, we’re not just thinking about the Mac,” he continued. “We’re thinking about the entire Apple experience across Mac AND mobile devices. That way, users can move seamlessly from Mac to iPhone to iPad without interrupting work— all while staying connected and productive.”

“We’re not just thinking about management,” said Strosahl. “Deployment is no longer the destination, but rather a step towards achieving a productive and safe workforce. We’ve expanded our capabilities to deliver integrated management AND security workflows so that your teams can focus more on delivering business outcomes with the confidence that your organization will meet IT and InfoSec requirements.”

“And we’re not just thinking about the traditional desk-bound worker,” he said. “Apple devices are used in many innovative ways across industries and around the world. The reason we are able to do all of these ANDs is because we focus on Apple. We’ve said many times 'when Apple innovates, Jamf celebrates,' and we follow their lead.”

Management, security, identity

Jeremy Butcher, Director of Product Marketing at Apple, joined us on the stage to discuss management, security and identity.

“We love seeing Apple devices being used every day at work and school,” said Butcher, “whether this is to teach a subject to a class or to enable and simplify business workflows.”

"We focus on three key pillars." He continued."Management, identity and security."

Managed Apple IDs

Managed Apple IDs provide access to various Apple services and are owned by an organization. They can be created manually in Apple Business Manager and Apple School Manager, or automatically using federation with an identity provider.

Butcher announced updates and improvements Apple is offering:

Expand access to iCloud services
Access Wallet, Continuity, and iCloud Keychain
Access management controls

Account-driven enrollments

"You can now sign in to enroll your device into management. We think that is a way easier, much more friendly way for the end user to actually enroll," said Butcher.

Apple users can enroll their devices using their Managed Apple ID directly from Settings and System Settings.

Zero-touch deployment

Butcher also announced new zero-touch deployment features:

- Require minimum OS version
- Enforce FileVault
- Enforce enrollment

"We're also bringing time and date update enforcement into the MDM protocol," said Butcher. "We're super excited to bring this into the protocol to make it easier to also tap into the operating system capabilities. So if you want to do something at 5:00, it's going to be done at 5:00, no matter where that device is located."

Management for watchOS

"Management is coming to Watch OS 10!" said Butcher.

With watchOS management, you can now:

- Manage iPhone and Watch together
- Enforce security settings
- Configure networking and per-app VPN
- Remote lock and erase

Jamf Nation was enormously pleased that Apple again sent a representative to talk to an excited JNUC crowd.

Manage and secure Mac and mobile

Sam Johnson, Chief Customer Officer for Jamf, discussed the necessary merging of management and security.

"Apple and Jamf couldn't be more aligned: management, identity and security!" said Johnson.

“The reality of the world we live in is that these concepts of management, identity and security are no longer in isolation,” said Johnson. “The lines of responsibility between management and security are fluid, and we have to find a balance. It is now the combination of these concepts together that allows you to provision and secure your end users. And after 21 years, we remain dedicated to just that.”

Jamf does this by offering the most comprehensive tools that work with the Apple platform across all devices: no matter who owns them, no matter where they are working and no matter what network they’re on.

Jamf is how you simplify work and embrace and extend the Apple platform for your organization instead of separating the endpoints by device type.

Trusted Access

Jamf’s ultimate destination? Trusted Access <https://www.jamf.com/solutions/trusted-access/>: Jamf management and security combined. A truly purpose-built, Apple-best, zero-trust solution.

Trusted Access means that users who gain access to sensitive applications and data must be:

Authorized users
On enrolled devices
Secure and free from threats

So let’s start down the road to Trusted Access by wiping the slate clean. To fully appreciate the outcome, we start with the device itself. And there has never been a more powerful tool to manage devices than Jamf Pro <https://www.jamf.com/products/jamf-pro/>.

Software Updates

Veronica Batista, Senior Manager in Product Marketing and Market Intelligence, took the stage to delve into Trusted Access.

Achieving Trusted Access starts, she explained, with a trusted device.

“Management is the foundation,” said Batista. "After all, you can’t secure what you can’t see.”

Most attendees to JNUC have already begun on the path to Trusted Access by using Jamf to enroll and automate their organizations’ device management.

Jamf Pro 11

“And we are always striving to make this better,” said Batista. As proof of this, Jamf recently released Jamf Pro 10.50: an exciting release that once again provided same-day compatibility for Apple operating systems.

Same-day compatibility with Apple OS’s

Same-day compatibility is important to Jamf because it is the best way to simultaneously protect our customers from unnecessary risk while also providing the best features and user experience possible.

“Same-day compatibility,” Batista continued, “has always been in our DNA.”

Realizing our vision

“We have a vision,” she said, “for how this should all come together. That’s why today we are taking that first important step on the path to a single Jamf platform experience.”

It all starts with Jamf Pro.

“Let’s say goodbye to Jamf Pro 10,” said Batista, “and hello to Jamf Pro 11!”

Jamf Pro 11’s new interface

“We’re so excited,” she continued, “to deliver this new version of Jamf Pro with an entirely refreshed user interface. This sleek and modern look complements the powerful workflows that only Jamf Pro can deliver, giving you a more versatile and enjoyable experience.”

The new interface also delivers important enhancements to accessibility compliance, including:

- Color changes
- Tab support for navigation elements
- Improved screen reader behaviors

“But the evolution of Jamf Pro is more than just a pretty face,” said Batista.

New shortcuts and automated workflows

Jamf Pro 11 offers easy shortcuts and automated workflows for many of the most popular Jamf Pro tasks:

- Guidance in creating a Smart Group
- Integrations with Slack and Microsoft Teams, allowing for notification directly in Jamf Pro
- Declarative Device Management

The ability for admins to schedule and enforce the latest software updates on managed devices by a specific date and time through Jamf Cloud
Automated device updates

Account-driven device enrollment

Jamf Pro 11 will also support Apple's recently announced enrollment workflow enhancements with account-driven device enrollment for macOS Sonoma and iOS 17. This enables users to easily enroll their institutionally-owned devices.

These enhancements offer a consistent enrollment experience with identity federation for your organization's cloud identity provider and prevent bad actors from pretending to be legitimate device enrollment sites to gain control of a device.

How account-driven device enrollment works with Jamf Pro

"Let's say," said Batista, "a device was procured by an individual department outside of formal procurement channels. If a user walks into the Apple Store and uses their corporate card, that device probably won't enroll through automated enrollment." In fact, IT may not even realize that the device exists— and that it may be accessing sensitive work resources.

Batista outlined the two options Apple users had in the past for enrolling a device into management: one, wiping the device and then sending the user through automated enrollment; unfortunately, that can hurt productivity. Two: directing users to an enrollment URL, which opens up a major risk vector.

Instead, Batista used an iPhone 17 to run attendees through the workflow that Jamf Pro supports today:

1. Navigate to settings
2. Sign in with work credentials
3. Follow guided enrollment steps that bring that device under management

The same workflow applies to macOS Sonoma, which Jamf will also support soon.

"This enrollment didn't require any special app or URL and the user didn't have any downtime," said Batista, "which allowed them to get right back to work."

And just like account-driven user enrollment, account-driven device enrollment maintains user privacy by separating personal and corporate data and apps on the device.

Onboarding

Coming soon in Jamf Pro 11: a simple, transparent Mac onboarding experience that allows users to monitor app installation progress while getting immediately to work. "With this new onboarding experience," said Batista, "we are able to show users information pertaining to Jamf apps, taking the first step in a journey toward unifying all Jamf experiences together for the user."

Jamf Cloud Distribution Service (JCDS) 2.0

Updates to JCDS will interest those who host different types of content such as packages, in-house apps and books.

Jamf’s new version of JCDS:

Increases performance
Makes uploading larger file sizes easier
Offers public API endpoints to programmatically upload, download and delete content

NEW: Jamf Remote Assist

> ***“When it comes to interacting with a remote device, easier is better. The integration within Jamf makes this process effortless . . .”***
>
> ***— Jonathan Krauet, Mac@IBM***

Jamf Remote Assist offers secure in-product remote screen sharing, allowing admins to assist end users on macOS devices with troubleshooting steps.

“When a user has a support issue,” Batista explained, “Jamf admins can securely initiate a Jamf Pro remote assist session, even when the user is not on the internal network. This is all within the Jamf Pro UI, making it easy and secure to remotely access and manage devices within their fleet.”

”We are excited to let you know that Jamf Remote Assist will be available later this year,” added Batista.

Visit <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275> <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275>the <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275> <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275>“Experience <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275> Jamf Remote Assist” <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275> JNUC session <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1694365222045001PRVc?_lab=3377700311770275> if you’d like to learn more.

First beta of Jamf Pro available

“I’m excited to announce that the first beta of Jamf Pro 11 will be available later today!” said Batista. “We expect this release to be generally available in October.”

Trusted users

Johnson then welcomed Linh Lam, Jamf’s CIO, to the stage.

"Good morning, Jamf Nation! I'm so excited to be back on this stage this year; you can feel the excitement!" said Lam.

“Establishing trust with enrolled, managed devices is the start of the journey to Trusted Access,” said Lam. “A trusted device should be complemented with a trusted user. Identifying the users across your endpoints and maintaining granular access controls around sensitive data is an essential component of Trusted Access.”

Identity-based workflows

“Apple has continued to expand identity-based workflows, like the enrollment workflows we just heard about in addition to simplifying access workflows,” continued Lam. “Jamf was early to support both Platform Single Sign-On (SSO) for the Mac and Enrollment Single Sign-on for BYOD mobile devices.”

These new workflows can be supported by any identity provider to deliver this next-generation SSO experience across Mac and mobile devices.

Platform SSO

End users access everything they need for work on a device with just one sign-on with platform SSO, which reduces login fatigue and improves productivity.

Enrollment SSO for BYOD

iOS users enjoy a fast and secure authentication with Face ID or Touch ID to access company apps on personally-owned mobile devices with enrollment SSO. This simplifies the account-driven user enrollment onboarding process while dramatically enhancing login security on BYO devices.

Jamf Connect legacy and Zero Trust Network Access (ZTNA)

“In 2018, Jamf introduced Jamf Connect <https://www.jamf.com/products/jamf-connect/> to solve a very real and prevalent access problem related to local Mac account management: Active Directory binding,” said Lam. “Jamf Connect has helped organizations around the world bring cloud identity to the Mac.”

In 2023, we face different access challenges as remote and hybrid workforces continue to grow and resources continue to be scattered across on-premises and cloud locations.

“This year,” said Lam, “Jamf Connect took the biggest leap forward in new functionality since its introduction six years ago: Jamf Connect now offers ZTNA.”

Jamf Connect can now securely route all of the data on a fully managed corporate-owned device with Jamf Trust installed.

Users can easily access their resources via browser or native app, and in stark contrast to many alternative solutions, the mobile experience is excellent as workers roam between networks and frequently reconnect to apps and email.

Jamf Connect enhancements

Lam also shared that Jamf will soon be enhancing Jamf Connect to automatically activate ZTNA upon deployment, ensuring that users have secure access to work resources from the moment they unbox a new Mac. Jamf also takes security a step further by protecting work traffic while your employees are working.

“This is really important,” said Lam, “because it’s not enough to just check that users have a secure connection when initiating a session. You need to ensure that *all* traffic with work resources is protected.”

Jamf’s focus on the best user experience combined with the highest security resulted in additional notifications for end users to inform them that a secure connection is required. ”The goal here,” said Lam, “is empowering users to return to secure productivity as quickly and easily as possible.”

The nuts and bolts of enhanced Jamf Connect for BYOD

For example, Jamf uses a per-app VPN that only applies to the work side of a BYOD device. “This means,” said Lam, “we can securely route and encrypt work traffic without having any visibility or control over the personal activities of the user.”

The BYOD user will see the per-app VPN light appear in the upper right when the Slack EMM app is opened. This indicates that the work app has a secure connection while respecting the user’s privacy by not routing any personal traffic.

SwiftConnect employee badge

Lisa Brown, Senior Director, Strategic Initiatives for IT at SAP <https://www.sap.com/index.html>, Kam Johnson, Access Partnerships at Apple <https://www.apple.com/>, and Brandon Arcement, CCO at SwiftConnect <https://swiftconnect.io/>, took the stage to explain an exciting development Jamf customers have been asking for: digital employee badges.

Apple Wallet <https://www.apple.com/wallet/> has become a natural part of the iPhone experience; purchasing with Apple Pay and storing digital loyalty, rewards and transit cards. It can now house an employee badge and key.

Kam Johnson led off with a brief background of Apple Wallet.

“Apple introduced Apple Wallet with a bold but straightforward goal,” said Johnson. “To digitize consumers’ wallets and allow them to seamlessly carry and easily use all of their cards, including payment cards, loyalty cards, tickets, boarding passes, health insurance cards, student ID, and keys, in a more secure and private way through iPhone and Apple Watch.”

In February 2022, Apple launched the ability to add employee badges in Apple Wallet, which allows users to easily access workspaces with their iPhone or Apple Watch.

Johnson introduced Lisa Brown, who came to JNUC to share some details about SAP’s employee badge in the Apple Wallet initiative and how SAP, SwiftConnect, and Jamf are working together.

“I’ve been involved from the start in the employee badge project at SAP,” said Brown. “Last year, I sat where you are today and I watched Linh show us how employee badges and Jamf Trust works for Jamf, and that demo inspired me. I’m very excited to say that we are rolling out our first Apple Wallet employee badges this month.”

Brown outlined some issues with physical access cards:

- They are easily lost or stolen
- Employees must visit a specific place to get an employee badge, which is often inside the very building they need access to
- Employees can forget to bring them to work

Employee badges added into an Apple Wallet, however:

- Keep everything secure on a worker's iPhone or Apple Watch
- Are available on demand; employees can provision employee badges themselves
- Are on a device very few people leave at home

Brandon Arcement filled the audience in on SwiftConnect: a SaaS platform that connects the many disparate parts of legacy keycard access control and facilities security infrastructure. This helps to bring businesses into the world of modern cloud applications, identity and technologies.

“In partnership with SAP and using the Jamf Trust app,” said Arcement, “we’re working to connect the broad range of SAP access systems, door readers, lockers, secure printers, and other employee services into one seamless credential in Apple Wallet.”

Arcement pointed out that with this addition to Apple Wallet, employees need only an iPhone or Apple Watch to access critical employee experience amenities. “On top of all of that,” added Arcement, “the Jamf Trust app will allow us to take this now dynamic digital credential lifecycle and link it to IT and InfoSec Trusted Access policies.”

Now, SAP can use device risk scores to discover if employee badges can be issued or not based on the device’s security state and if it meets corporate InfoSec requirements.

“One thing I want to make sure I add,” continued Arcement, “is that employee badges in Apple Wallet is without a doubt an employee experience driver. Our customers constantly tell us about how often their employees comment on the ease of use, security and overall delightful experience of using their iPhone or Apple Watch to gain access to their corporate facilities.”

Partner highlight: Jamf and Google

Prashant Jain, Head of BeyondCorp <https://cloud.google.com/beyondcorp> Strategic Partnerships at Google, joined Sam Weiss, Alliance Partner Manager at Jamf, to discuss some of the remarkable strides that Jamf and Google’s collaboration has taken in the past year.

BeyondCorp

The traditional security perimeter is no longer sufficient in today's dynamic work environment. BeyondCorp, Google’s zero-trust framework, is shifting focus from the network and toward the user and their device. This allows for more secure access to company resources from anywhere and integrates seamlessly with Jamf Pro, ensuring that only trusted devices have access to critical systems—regardless of location.

"Jamf helps deliver a phenomenal, secure Apple experience for organizations that rely on Google Cloud and Google Workspace," said Sam Weiss. “Jamf's focus helps integrate and extend these Google products to users of Apple hardware in ways that make the most of both ecosystems.”

"This year,” said Prashant Jain, “we’re proud to partner with Jamf to extend BeyondCorp and Context-Aware Access protection to iPhone and iPad. Now Jamf can send compliance status for all the managed mobile Apple devices in your fleet, in addition to the macOS support we launched last year.”

"Jamf is excited to be the first BeyondCorp Alliance partner to integrate Mac and mobile Apple devices into the Google Cloud Security ecosystem," said Weiss.

View “Jamf <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1678477938211001K3aE?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275> and Google: Leveraging BeyondCorp for Zero Trust Across the Entire Apple Ecosystem <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1678477938211001K3aE?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275>” to learn more about Jamf and BeyondCorp.

Chronicle

Jamf Protect <https://www.jamf.com/products/jamf-protect/> and Google’s security operations platform, Chronicle <https://marketplace.jamf.com/details/google-chronicle>, now integrates with Jamf to provide comprehensive Apple security visibility for Google Chronicle customers.

“With Jamf Protect's advanced Apple threat detection capabilities combined with Chronicle's powerful data correlation, enrichment and security analysis, businesses can rapidly identify and respond to potential threats in their Apple environments. You can leverage the rich contextual insights provided by this integration,” said Jain. “The integration enables IT and security teams to gain the upper hand in safeguarding their organization from cyberattacks.”

Chrome Enterprise browsing

”Google and Jamf’s work together is all about creating an exceptional Apple experience in the Google-equipped workplace,” said Weiss.

And Chrome Enterprise browsing takes the user experience to a new level.

”Chrome Enterprise offers a seamless and secure way for you to browse,” said Jain. "It’s in aligned with the needs of security and IT teams, and the ease-of-use that end users need."

Organizations can now offer employees the performance and security of Chrome while also managing and configuring browser settings easily.

“Jamf has made it simple to enroll browsers into Chrome Browser Cloud Management, and we’ve made incredible strides to make it an even more powerful security ecosystem,” said Jain.

New features include sending critical security event information from Chrome to:

- Chronicle
- Splunk
- Okta

Learn more by visiting the “Secure <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1690816568436001C7Cn?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275> Enterprise Browsing with Google Chrome and Jamf <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1690816568436001C7Cn?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275>” or “Take <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1677686675249001Y1Dz?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275> your Chrome Browser Management to a New Level - Basic to Advanced with Jamf Pro and Jamf School <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1677686675249001Y1Dz?_lab=1147214525&utm_campaign=manage-secure&utm_content=2023-06-02_protect_&utm_medium=brochure&utm_source=downloadablecontent&_lab=3377700311770275>” sessions.

Protected endpoints

The power of Jamf is that it seamlessly integrates with Google, MS, Okta, etc. But you can also add to that or cover a lot of bases, all within Jamf. Michael Covington, VP, Portfolio Strategy at Jamf, took the stage to explain more.

“At Jamf,” said Covington, “we believe that the Apple platform offers not just the best end-user experience but the most robust foundation for handling sensitive business data. And yet there still remains several misconceptions about securing your Apple deployments.”

Organizations, he pointed out, must still be intentional about how they secure endpoints and prevent threats on Apple devices, just as they secure all endpoints.

“For Jamf, we believe that security should never be a bolt-on or an afterthought,” continued Covington. “And we don’t dilute your security posture or user experience by pursuing a lowest common denominator approach to endpoint security. We work tirelessly to expose all of the rich security capabilities that Apple frameworks enable.”

Jamf Compliance Editor

For most organizations, one of the very first security objectives they have with any new platform is compliance. “We’ve heard from our customers that understanding, defining and maintaining the various settings required to actually make your Mac fleet compliant with, say, CIS benchmarks, NIST 800 or DISA STIG can be really difficult.”

The challenge: to properly configure the required benchmarks, customers often have to implement over a hundred settings. Configuration profiles can’t set many of these benchmarks.

“Thanks to the macOS Security Compliance Project <https://support.apple.com/guide/certifications/macos-security-compliance-project-apc322685bb2/web> and Jamf Compliance Editor <https://trusted.jamf.com/docs/establishing-compliance-baselines#jamf-compliance-editor>,” said Covington, “this work can now be accomplished easily, in record time, with a high degree of confidence. In fact, we even provide the receipts.”

The macOS Security Compliance Project is an open-source effort that works to update compliance baselines for each upcoming macOS version so that organizations can maintain compliance while also pursuing same-day support for the latest macOS release.

Jamf Compliance Editor integrates directly with the macOS Security Compliance Project to pull guidance for all of the supported benchmarks. Jamf Compliance Editor will upload all of the required configurations and scripts to Jamf Pro while also providing full documentation that you can hand to your compliance team.

Compliance dashboard

“Of course, compliance isn’t just about setting it and forgetting it,” said Covington, citing the fact that organizations must monitor their compliance statuses continuously to ensure all endpoints remain configured correctly. “This can be a difficult thing to stay on top of, which is why I’m excited to announce that a brand new compliance dashboard is coming soon to Jamf Protect <https://www.jamf.com/products/jamf-protect/>.”

This new dashboard will offer a new view of business compliance based on organizational compliance rules. It will allow customers to easily identify and resolve the highest-risk areas across their environments.

“And soon,” added Covington, “we’ll also be offering new workflows to define pragmatic compliance rules within Jamf Protect that can be converted to actionable guidance with Compliance Editor and deployed across your entire fleet with Jamf Pro.”

Device vulnerability

This builds upon and extends Jamf Protect’s existing vulnerability management dashboards. With vulnerability management, customers can view the overall health of their fleets, based upon known Common Vulnerabilities and Exposures (CVEs) of various operating systems and app versions.

“Keeping track of all published CVEs across all apps and operating systems in your environment can be very tedious and time-consuming,” said Covington. “Thanks to Jamf Protect, you get a simple breakdown of your overall vulnerability distribution with access to granular details about specific vulnerabilities and risky devices.”

Jamf helps teams make well-informed decisions regarding access policies and patching priorities, all to mitigate risk from potential CVE exploits in their environments.

Inbound threats

As the Apple platform gets more attention from the enterprise, it gets attention from hackers, as well. Beyond the risk associated with CVEs, it’s also important to prevent the wide array of inbound threats that face users daily.

“Just this year,” said Covington, “we’ve seen the first viable ransomware designed specifically to attack macOS. We’ve witnessed the development of sophisticated cryptojacking malware that targets Apple silicon."

Covington especially underscored the importance of phishing protections as they remain the leading threat facing users. “The simple truth is,” said Covington, “that security awareness training is important but alone, it is insufficient to mitigate the risk. Users are busy, phishing attacks continue to evolve, and are so much more difficult to identify by mobile users."

The good news? Phishing protection is built into both Jamf Protect and Jamf Safe Internet <https://www.jamf.com/products/jamf-safe-internet/>, stopping threats in their tracks and giving users clear guidance when they encounter risky content.

Jamf Threat Labs

“Although there are a lot of bad actors out there, I’m very proud to highlight the great work that Jamf Threat Labs <https://www.jamf.com/threat-labs/> has contributed to Apple platform security,” said Covington, “including having multiple vulnerability discoveries attributed to them in the last couple of years. Jamf Threat Labs have made a significant dent in understanding the overall threat landscape."

Jamf’s team of security researchers works tirelessly to identify all manner of threats that target Apple users.

Jamf Executive Threat Protection

When people hear about Jamf Protect or Jamf Threat Labs, they usually associate that with Jamf’s unparalleled visibility and security for Macs.

When it comes to mobile devices, however, there aren’t a lot of options for that same deep level of insight due to the sandboxed and secure nature of iOS.

Last year, Apple introduced Lockdown <https://support.apple.com/en-us/HT212650>M <https://support.apple.com/en-us/HT212650>ode <https://support.apple.com/en-us/HT212650> as an additional layer of protection for users who might be personally targeted because of who they are or their access to specific information.

“While Lockdown Mode does reduce the attack surface of your device,” said Covington, “security teams still need supplemental visibility to assess the integrity of a mobile device and to understand what happened on a compromised device. Security teams have told Jamf that they require more."

Earlier this year, Jamf introduced Jamf Executive Threat Protection <https://www.jamf.com/resources/press-releases/jamf-launches-jamf-executive-threat-protection/>: an advanced detection and response solution for mobile devices. It gives organizations a powerful and remote method to understand what has happened on their mobile devices, as well as tools to respond to advanced attacks.

Although these sophisticated attacks are highly targeted and less common for the average user, the risk associated with device compromise is significant. “Jamf Executive Threat Protection offers unmatched mobile endpoint telemetry and a security engine that synthesizes all of that telemetry,” said Covington. Users can then identify the breadcrumbs of an attack, and if a user’s device has been compromised, security teams will have all of the tools required to quickly identify and remediate a compromised mobile device.

“Hopefully you’re able to see how our intense focus on Apple platform security makes Jamf the preferred endpoint security solution for your Mac and mobile devices,” added Covington. “The broad array of endpoint security data signaled across the Jamf platform is the reason why our Trusted Access solution is so responsive and so secure.”

And thanks to the rich integrations available with partner solutions, organization technology stacks can access all of these Apple-best insights.

Partner highlight: Jamf and Microsoft

Naadia Sayed, Principal Product Manager at Microsoft Security, stepped up to discuss security for all.

“Now, some of you might be wondering what a Microsoft person is doing at a conference for Apple admins,” said Sayed. “Well, let me tell you, attackers don’t care what device or operating system you are on. At Microsoft, we believe in security for all.”

Microsoft’s research has shown that there are 4,000 password attacks globally *per second.* “That makes security a team sport,” said Sayed.

The Jamf team has developed integrations with Entra ID and Microsoft Sentinel for Office 365 users.

Entra ID

“As you may know,” said Sayed, “we rebranded Azure Active Directory to Microsoft Entra ID. Microsoft Entra is our family of Identity and Network access products that help address security challenges that come with increasing attack surfaces.”

The Jamf Pro integration, explained Sayed, improved admin ability to:

Share compliance data with Microsoft Intune
Enforce conditional access criteria
Offer remediation paths

This means that Apple device users set up with Entra ID authentication enjoy automated compliance management.

“Our customers are asking for zero-trust device compliance,” said Sayed. “You, our IT admins, can now establish compliance criteria to ensure devices meet security standards before accessing organizational resources.”

Microsoft uses device information Jamf collects to evaluate device compliance before sending traffic to Entra ID and grants access to Office 365.

"We have worked closely with Jamf to dramatically improve the device compliance onboarding user experience,” said Sayed.

Microsoft Sentinel

Microsoft Sentinel <https://marketplace.jamf.com/details/jamf-protect-for-microsoft-sentinel> allows Microsoft customers using Apple products to automatically forward macOS activity, malicious attacks, and malware notifications directly into existing Microsoft Sentinel workflows and dashboards.

What’s on the horizon for Jamf and Microsoft?

“Last year at JNUC,” added Sayed, “there was a lot of talk about Platform SSO for macOS. We heard your feedback loud and clear, Jamf Nation! Enterprise SSO is now generally available with Microsoft Enterprise SSO plug-in for Apple devices <https://learn.microsoft.com/en-us/azure/active-directory/develop/apple-sso-plugin>.”

Sayed also announced that Microsoft teams are working on a powerful enhancement called Platform SSO for macOS, which will be in public preview in the upcoming months.

This integration will streamline authentication and improve security by further simplifying the device compliance onboarding process.

Trusted Access login and training for in-person JNUC attendees

Sam Johnson thanked Naadia Sayed as he joined attendees to explain more about Trusted Access.

“As you can see,” said Johnson, “this is how we deliver Trusted Access: our zero-trust vision of Apple at work.”

“This is really a story of how Jamf Pro, Jamf Connect and Jamf Protect work together to deliver the most delightful and secure workplace experience across different device types,” said Johnson. “It’s the culmination of management, identity and security working together at their best.”

JNUC attendees: experience Trusted Access at JNUC

Johnson shared an exciting announcement to those in-person JNUC attendees: Jamf is providing a login and training so that admins can test the full Jamf platform -- regardless of what product they own.

Customer highlight: Secrid

Sam Johnson was pleased to welcome Sander Schram from Secrid <https://www.secrid.com/>, a family-owned Dutch company that makes RFID-secure wallets in a socially responsible manner. They chatted about Secrid's journey to Trusted Access.

An Apple shop with far-flung employees

Secrid uses mainly macOS computers and iOS mobile devices at every level of the organization, as well as in their brand store in Rotterdam. Some work from the organization's headquarters in the Netherlands, some remotely from home or while traveling.

"Our journey with Jamf started with the implementation of Jamf Pro to manage the deployment of software, settings and policies to our growing number of Apple devices," said Schram. After a full deployment of Jamf Pro, Secrid implemented Jamf Connect, and they use Okta as their IdP.

Jamf also makes it easy and safe for Secrid to implement iPads for point-of-sale in their brand store in Rotterdam.

Reaching Trusted Access

"We wanted modern and secure authentication for our Mac devices," said Schram. "This gave our users a great zero-touch enrollment experience and they could authenticate to their devices with just one source of authentication; Okta."

After a consequential phishing attack, last year the organization implemented Jamf Protect, which Schram believes would have prevented the attack had it been in place at the time. ”Training and educating our users was not good enough," said Schrma. "The impact was enormous, mostly because of the amount of hours we spent on communication with the involved companies and parties but also reporting the GDPR data breach incident to the Data Protection Authority (DPA)."

Security wins with Jamf

"This spring," said Schram, "there was a security incident with the software of our VoIP solution, which Jamf Protect was able to quickly detect, block and remediate."

"We've even had a few attempts to steal our iPads at our retail location," Schram said. "But with Jamf, we were able to lock these devices down and prohibit any access to sensitive information."

In addition, Secrid is saving time, effort and cost with the full Jamf offering. "All the devices," said Schram, "no matter where they are located, are always secure and trusted."

What’s next for Secrid?

“As we sat in the JNUC audience last year and heard about your partnership with SwiftConnect to make physical access a reality,” said Schram, “we are extremely intrigued by the possibility of bringing this level of digital protection to our physical buildings.”

Jamf improvements for education

Mat Pullen, Jamf’s Senior Product Marketing Manager, Education, joined the audience to catch educators up on Jamf’s ongoing commitment to education. Jamf, which started at the University of Wisconsin-Eau Claire, believes that a strong educational framework, equitable access to resources, stellar educators, and best-in-class educational technology can shape who we become as adults and leaders.

“iPad and Mac in education are devices that all serve a purpose,” explained Pullen. “The purpose of these devices is to teach and learn.” The core purpose? To transform teaching and learning, not to increase personal productivity as with Mac and iPhone.

On-Device Content Filtering for Jamf Safe Internet

Jamf recently launched Jamf Safe Internet: a robust content filtering and mobile threat solution to ensure students only access safe and approved resources on the internet. It now supports Apple, Chromebook and Windows devices.

“But we’re not done there,” said Pullen. “Let’s talk about a few new and exciting tools we're bringing to help complement that solution."

With the adoption of Apple’s network-filtering framework, Jamf further protects schools and districts with web protection enforcement that is directly on Apple mobile devices. On-device content filtering bolsters existing security measures by strengthening web filters for schools. It stops both inbound threats and unsafe outbound activity while ensuring greater privacy for students.

“You may be wondering: ‘Don’t existing content filtering solutions already do this?’” said Pullen. “Yes and no. Traditional content filtering methods are a great place to start, but by adding on-device content filtering we're offering additional layers of security and extra privacy protections.”

These additional protections safeguard against:

- Phishing
- Social engineering
- Credential theft

Jamf’s on-device content filtering is part of Jamf Safe Internet and is currently available for supervised iOS and iPadOS 16+ devices. Jamf is planning macOS support for on-device content filtering later this year.

StateRAMP status: Ready

The rise in ransomware and cyber threats to schools has increased dramatically over the last few years.

With this in mind, Jamf has achieved StateRAMP status 'Ready,' and can now deliver StateRAMP instances of Jamf School and Jamf Pro to US schools. StateRAMP is a non-profit organization that promotes cybersecurity best practices for public institutions. While StateRAMP is a US-focused initiative, this benefits to all of our customers as Jamf focuses on high-compliance models.

"If you are interested in taking on a StateRAMP instance," said Pullen, "we will provide you with the necessary information you need to get the migration going. Best of all, there is no need to re-enroll your devices."

Usability improvements for Jamf School

Jamf School has added usability improvements for Jamf School beyond the new interface outlined by Veronica Batista.

"We are proud to serve a large community of educators with our education solutions," said Pullen. "We know that Jamf Teacher is a tool they love to use daily to help them transform teaching and learning, including the ability to maintain contact with the restrictions you have in place for your learners," said Pullen.

Jamf Teacher users can now see all student restrictions as well as the time left on those restrictions. This enables teachers to add or remove any of those restrictions without having to reset the whole system.

App Installers for Jamf School

"Oh, and one more thing," added Pullen. "We bringing the most requested feature to Jamf School: App Installers." Available today, this adds the functionality currently available on Jamf Pro to Jamf School and provides educators with a more complete Mac management experience.

Customer highlight: Mesa Community College

Alvin Bridges, Associate Vice President for College Technology Services at Mesa Community College <https://www.mesacc.edu/>, joined Mat Pullen to discuss how Jamf has helped his school. It is the largest non-statewide local community college district in the nation, with ten sister colleges. The school has implemented a 1-to-1 iPad program and Bridges secures the college's data and network with Jamf Protect and Jamf Safe Internet.

Why?

"Jamf is just easy to use," he explained. For instance, when the college received an executive order from the governor to block a certain social media site, "We were up and compliant in four hours," said Bridges.

"The successes of our iPad program have been monumental," said Bridges. "48% of our students are first-generation college students. One student thought he wasn't going to finish school until he discovered our iPad program. He is now in his third semester."

The college secures their devices with both Jamf Protect and Jamf Safe Internet: Jamf Safe Internet to ensure appropriate access and to protect their network, and Jamf Protect to secure data and apps on each device.

What's coming next for Mesa Community College?

"We are going to expand our program to 80,000 students," said Bridges. "We continue to work tirelessly to close the digital equity gap."

Customer highlight: Richardson ISD

Morgan Cave, Director of Instructional Technology at Richardson ISD <https://web.risd.org/home/>, spoke to the audience about her school's successes with Jamf.

They use Jamf Pro to manage 30,000 mobile devices and 5,000 Macs for students and teachers.

"When I first started teaching," said Cave, "I wanted most for my students to love the experience of learning." Her classroom was completely transformed in 2013 when the campus introduced a 1-to-1 iPad program. "I saw how iPad created pathways for my first-grade writing and language students," said Cave, "And my fifth-grade classroom found that the creative capabilities of iPad reignited their love of learning."

However, Cave's lesson prep meant touching 85 iPads after school. "That's why I very much understand the value of Jamf Pro!" Cave said.

Cave particularly values the guidance that Jamf provides. "Working with our engineer," she said, "we can understand the instructional implications of every configuration and all of the possibilities to customize and personalize for our users."

Last year, the schools needed access to new iPads. "We refreshed 20,000 iPads in January 2023," said Cave. Not only was the refresh fast and seamless, but using enrollment configuration resulted in little to no loss of instructional time. "Students signed back into their devices and picked up right where they left off," she added.

They turned over entire campuses in one day, and sometimes in a few hours.

"Our students are challenged to think critically and use technology to solve problems as they creatively apply learning and demonstrate mastery," said Cave, adding: "Jamf Teacher allows our teachers to design engaging learning experiences that align with district initiatives."

Jamf Teacher started testing in two classrooms, and now all 41 elementary campuses are using Jamf Teacher. "Since starting with Jamf Teacher," said Cave, "Our teachers feel confident and empowered with technology and they can stay focused on what matters most: teaching and learning."

AI’s role in device management and security

Akash Kamath, Senior Vice President, Engineering, Jamf, stepped up to tackle the sometimes controversial topic of Artificial Intelligence (AI).

“AI has become a buzzword in the tech industry today,” said Kamath. “We have all heard the prophecies ranging from AI saving us all to AI taking over the world.”

Kamath invited the audience to pause for a moment and cast their minds back to the origins of computers and the role they have played in the popular unconscious.

”50 years ago,” said Kamath, “computers were enigmatic machines, confined to labs, touched only by the lab-coated elite.” Then, in 1984, “the heavens split open, and down came the Apple Macintosh,” he continued.

The Apple Macintosh wasn’t just a computer. “It was a bicycle for your mind, an invitation to dream,” said Kamath. Just as the Mac removed barriers between humans and computing, Kamath argued, generative AI makes artificial intelligence personal.

“It takes it out of the hands of the few and places it into the hands of many,” he continued. “It's not some far-off theoretical future; it's here, now, shaping our world in ways we're just beginning to grasp.”

“It's impossible to ignore the seismic shifts AI is causing across industries,” said Kamath. For instance, McKinsey's “Generative <https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america> AI and the future of work in America <https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america>” report predicts that by 2030, generative AI could be behind the automation of nearly one-third of all work hours.

“That's a game-changer,” said Kamath, “but let's not forget the cautionary examples like ChatGPT's ‘hallucinations,’ which can lead to misinformation. This is particularly alarming for us at Jamf, where we believe that 'Trusted Access' isn't just a tagline—it's a commitment.”

Jamf Collaboratory

“So how do we harness the unprecedented capabilities of AI without compromising the trust you place in us?” asked Kamath. “That's the question that led to the creation of the Jamf Collaboratory: a cross-functional internal team of visionaries, tinkerers and problem-solvers. We aren't just dabbling in algorithms; we're pioneering a new era of intelligent solutions meticulously crafted to enhance Apple device management and security.”

“I'm thrilled to give you a sneak peek of what we're actively developing,” said Kamath.

One cornerstone project: a specialized language model that marries the capabilities of state-of-the-art large language models with proprietary data, derived from Jamf Pro documentation and insights gleaned from Jamf Nation user forums.

A model intentionally shaped to grasp the complexities of Apple management and security, this adapted language model will serve as the foundation for a series of future innovations.

One example: an admin wants to schedule a policy to run at a specific time of day. Is this in our standard documentation? “When we posed this question to ChatGPT,” said Kamath, “it fabricated a ‘schedule tab;' something that doesn't exist.”

Jamf Help presents two viable solutions: first, using client-side limitations in policy configuration. If that doesn't suffice, Jamf Help offers a step-by-step guide to creating a launch agent for timely policy execution.

If an admin wants to query an SQL database for each endpoint during inventory updates, Jamf Help will provide a hands-on tutorial for crafting the necessary extension attribute.

“We're encouraged by the early results from Ask Jamf but acknowledge there's room for improvement,” said Kamath, inviting attendees to visit the Jamf station in the expo center to test it for themselves and to offer insights.

“Our aspirations don't end with a language model,” said Kamath. “The ultimate goal of AI integration into Jamf products is to function as a silent partner that amplifies your effectiveness.”

Organizations today are under pressure to maximize efficiency, often expecting IT professionals to wear multiple hats. “One significant shift we've noticed is the increasing expectation for IT staff to manage cybersecurity tasks, especially for endpoints, in addition to their day-to-day operational responsibilities,” said Kamath. “This can be a tall order, particularly when many IT professionals lack specialized cybersecurity training.”

Even mature information security teams often lack the expertise or bandwidth to keep up-to-date on Apple security. IT is often deluged with security alerts and vulnerabilities that they may not be fully equipped to navigate.

“In a world where one missed alert could spell catastrophe for your organization, what you need is both efficiency and precision,” added Kamath.

Kamath then outlined a few scenarios in which AI would be very useful in an admin’s workday by sharing some ideas the Jamf team is currently working on.

First: an employee is duped into running a counterfeit version of Google Chrome designed to harvest login credentials. Second: a coworker pranks another by directing them to execute a harmless command in their Terminal.

“Here’s the paradox,” said Kamath. “If you're using Jamf Protect, both of these scenarios trigger alerts that look nearly identical. Distinguishing between them demands expertise and time—luxuries that most of us don't have.”

Hypothesis

"We are experimenting with a hypothesis function with Jamf Protect," said Kamath. "It leverages the collective insights from Jamf threat labs and the capabilities of Artificial Intelligence to instantaneously analyze an event and its associated telemetry data." Then, the hypothesis feature will issue a comprehensive, three-dimensional view of the situation. It will offer explanations and evidence used in its analysis, along with tailored suggestions for further investigation and remediation.

“In essence,” says Kamath, “This function acts like an additional member of your security team, adeptly helping you separate the critical from the benign.”

For an in-depth look at this feature, view “Hypothesis: <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1691770739718001Uz76?_lab=3377700311770275> GenerativeAI at Jamf <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1691770739718001Uz76?_lab=3377700311770275>.”

“Your roles in IT and InfoSec are rapidly evolving,” said Kamath, “and we're committed to evolving right alongside you. Intelligence-backed management, endpoint security, and a more streamlined workflow are not just catchphrases; they are our collective future. We invite you to be a part of this journey by sharing your invaluable insights, challenges, and aspirations. Let's continue to push the boundaries of what's possible together.”

Enterprise technology choice

Sam Johnson took the stage to talk about the many organizations that have partnered closely with Jamf to speak up about enterprise technology choice. Upfront cost, Johnson argued, isn’t a good reason for passing on Apple.

He reminded attendees that at JNUC 2015, Fletcher Previn of, at the time, IBM, asked: “When did it become OK to live like the Jetsons at home but the Flintstones at work?”

“Well,” said Johnson, “Fletcher's back, baby." Now as the CIO at Cisco, Previn continues to ask that question. And once again has validated the cost, time and resource savings of allowing employees their choice in hardware.

Previn will be presenting much more insight and data during his “Mac <https://reg.jamf.com/flow/jamf/jnuc2023/home23/page/sessioncatalog/session/1689018711125001U1b9> in the Enterprise: a CIO’s Perspective by the Numbers <https://reg.jamf.com/flow/jamf/jnuc2023/home23/page/sessioncatalog/session/1689018711125001U1b9>” session.

“But IBM and Cisco are not the only choice programs Jamf has helped spearhead,” said Johnson. “We are getting into the rhythm of it by now. Enterprise juggernauts like SAP and HSBC are also on the record dispelling the notion that Mac is too expensive."

These numbers show that you *can* have the best hardware at the lowest cost.

Trusted Access: Jamf’s present and future

Jamf CEO John Strosahl rejoined Jamf Nation to get the day started.

“Simply said,” Strosahl explained, “Trusted Access is an outcome you can achieve when you Manage and Secure your Mac and Mobile devices with Jamf, regardless if it's deployed for a person or for a purpose.”

“I’d like to thank all of our presenters,” continued Strosahl, “and our sponsors for making this a keynote and JNUC to remember. A special thank you to our premier sponsors AWS and Insight.”

JNUC 2024

Strosahl then revealed the location of JNUC 2024: Nashville, Tennessee.

“Take care, Jamf Nation,” said Strosahl. “I look forward to connecting with you this week.”

Watch the entire keynote presentation.

View Keynote <https://reg.rainfocus.com/flow/jamf/jnuc2023/attendee-portal/page/sessioncatalog/session/1686588285158001ha8p?_lab=3377700311770275>

Haddayr Copley-Woods
Jamf

‹ **Previous Blog Post:**
Prev
What does same-day support really mean and why is it so crucial? <https://www.jamf.com/blog/what-does-same-day-support-really-mean/> **Blog Homepage**
<https://www.jamf.com/blog/> **Next Blog Post:**
Next
What’s next for MDM? › <https://www.jamf.com/blog/declarative-management-in-mdm-with-jamf/>