Jamf Nation User Conference showcases Jamf's new and upcoming product innovations that will help organizations simplify and secure work

September 27, 2022

Jamf now powers over 69,000 active customers on more than 29 million devices

MINNEAPOLIS, Sept. 27, 2022 (GLOBE NEWSWIRE) -- Today, Jamf (NASDAQ: JAMF), the standard in Apple Enterprise Management, kicked off its 13th annual Jamf Nation User Conference (JNUC) both virtually and in-person in San Diego, California. Joined by partners including Apple, Google, Okta, Microsoft, Amazon Web Services and SwiftConnect, Jamf shared how its continuous product innovation is helping organizations succeed with Apple in a rapidly evolving work environment.

"The focus of this year's JNUC is simplifying the management and security of devices used for work. In order to do this, we are asking Jamf Nation two questions: do your users love the technology they are using for work, and do your IT and security teams trust that technology? Our focus at Jamf is to ensure the answer to both of those questions is a resounding 'yes', with something we call Trusted Access," said Dean Hager, CEO of Jamf. "Trusted Access puts enrollment at the foundation – whether for a BYO or corporately-owned device – and establishes the user as trusted. It also ensures only safe devices are able to access work resources to keep company data protected. For those devices that are enrolled and safe, their access to resources is completely seamless. The user can work anywhere, access all the corporate resources they need, and do not require multiple passcodes to remain productive."

Key highlights of JNUC 2022 include:

A new way to BYOD
Bring your own device (BYOD) programs have gained even more traction over the last two years, as the lines between work and home technology blur and more work is done on mobile devices. After rolling out a new BYOD offering earlier this year, Jamf kicked off JNUC by demonstrating their own internal deployment for BYOD devices all built on Jamf and Apple-specific workflows. These features are intended to eliminate the common practice where employees carry two mobile phones — one for work and one personal. Key capabilities of this new workflow include:

- Employee self-enrollment and setup with no action needed from IT
- Device partitioning for secure work with a separate partition for personal privacy
- Cloud identity-based single sign-on for all work applications and access to corporate data
- Self-Service app installations with app-based security automatically set up
- Next-gen cloud VPN private access to enterprise resources with no setup required by users
- Automatic zero-trust blocking of all compromised users and devices
- Enterprise ID cards procured and placed in Apple Wallet for access to physical offices
- Simple workflows to setup dual eSims, supporting one work phone line and one personal
- Apple's Focus mode to transform BYOD iPhones to work-only or personal-only for better work life balance

Device security out-of-the-box
The unboxing and onboarding experience is an important one, especially today as more and more employees sign in for the first time from home. Jamf has taken zero-touch deployment to the next level, providing a simple experience that users love. Jamf-managed Apple devices can be shipped directly to an end user, ready for automatic configuration for an individual's use and fully secured against on-device and in-network security threats from the moment the device is powered up for the first time.

Jamf's endpoint security suite can now ensure macOS and iOS devices are configured correctly and secured against cyber attacks from first boot with a new app called Jamf Trust. The Jamf Trust app binds user identity to the device so that Jamf's security services are dynamically configured according to user identity and role, and carried through to their application access, streamlining the need to enter credentials and verify identity.

Additionally, next month Jamf Protect will gain rich endpoint telemetry data collection along with a new offline deployment mode that streams telemetry data directly to a SIEM for customers with high compliance requirements.

Just in the last 12 months, Jamf has scanned more than 430 million unique domains. By measuring a multitude of dimensions of these sites, including top-level domains, subdomain entropy, domain compositions and brand impersonation, Jamf has been able to identify and block more than 122,000 zero-day phishing attacks just in the last year.

Yesterday, Jamf announced it signed a definitive agreement to acquire ZecOps, a leader in mobile detection and response. The acquisition uniquely positions Jamf to help IT and security teams strengthen their organization's security posture through an app that detects indicators of compromise on mobile devices, accelerating a mobile security investigation from weeks to minutes, and on a much deeper scale.

Always updated software

For the past two decades, Jamf has provided same-day readiness with new Apple operating systems. Last year at JNUC, Jamf tackled an additional software problem for users and IT administrators: keeping apps updated. With the introduction of App Installers within the Jamf App Catalog, Jamf made third party software updates for macOS, which constitutes 80% of all Mac apps run by Jamf customers, as simple as App Store updates.

At this year's JNUC, Jamf announced it has grown its monitored software to over one thousand titles, and now offers more than one hundred App Installers designed to substantially lower the work effort for IT while improving the security posture of an organization's fleet of devices. App Installers are pre-vetted and maintained (patched, updated, monitored for risk) over the lifespan of the device.

Jamf also announced new App Installer features to be delivered in the near future, including improved user notifications and simplifying App installation within Self Service to ensure only apps relevant to the user and authorized by IT are displayed in their customized app catalog.

Multi-layered zero trust access
Jamf has taken its patented Smart Group technology to the next level by synthesizing multiple layers of data including user, device and new risk data into powerful security workflows that allow organizations to identify threats and take action on that information automatically.

With Jamf's unmatched Apple device inventory and controls, Jamf is able to block access to Apple devices or specific capabilities on the device when a compliance issue has been detected. Additionally, working with cloud identity providers like Okta, Jamf can now enforce use of Private Access to ensure only protected devices with encrypted data can run enterprise apps, while automatically blocking compromised users and devices.

Furthermore, Jamf announced deeper integration with leading Cloud providers Microsoft and Google.

- *Microsoft Device Compliance:* The next generation of the Microsoft Device Compliance integration will be available for macOS later this year, a technology currently available on iOS, which will align the full power of Microsoft Device Compliance consistently across all Apple devices. This new workflow will allow admins to fully define compliance with any Smart Group criteria, including the newly added device risk score.
- *Google BeyondCorp:* Jamf will also be supporting BeyondCorp, Google's context-aware zero trust framework on iOS devices in early 2023, an integration that is currently available to Jamf customers on Mac.

The combination of these new zero-trust capabilities provides multiple layers of organizational protection by using device health scores and Smart Groups to block non-compliant usage at device, network and cloud layers.

Modernized access to the physical workspace
Plastic access badges to office spaces will soon be a thing of the past. Earlier this year, Jamf enabled employee badge in Apple Wallet so that its employees could conveniently and securely access Jamf offices with just a simple tap of their iPhone or Apple Watch.

Jamf and SwiftConnect are working together to allow businesses to seamlessly enable employee badges in Apple Wallet for their organizations in the near future.

Unmatched visibility into Mac fleet
Jamf is ready to provide support for Apple's new Declarative Device Management functionality. This means the device will proactively report its status in real-time and then action can be automated or user-driven to get the device into a new state for security, compliance or productivity reasons.

Additionally, as announced last week, Jamf and AWS showcased their new partnership to automatically enroll virtual EC2 Macs into Jamf Pro when they are provisioned through the AWS portal. This provides IT administrators visibility into the entire Mac fleet — both physical and virtual. Additionally, administrators can now use Jamf to deploy policies, configurations and software to their virtual Macs while collecting a full complement of inventory details about the computer and the EC2 environment it's running in.

Delivering in early 2023, Jamf announced a new Remote Access feature that will empower IT admins with the ability to authenticate and take remote control of any Mac in their fleet — both physical and virtual — directly from within Jamf Pro. In a hybrid work world, this capability substantially improves IT's ability to support users and devices anywhere in the world.

Empowering students while keeping them safe
Launched earlier this year for macOS and iOS, Jamf Safe Internet ensures students have a safe and secure online learning environment from the moment they unbox their device. This online student safety product is coming soon to Chromebook and Windows devices in early 2023. Earlier this month, Jamf added support for Google Safe Search and YouTube restricted mode within Safe Internet giving organizations more robust control over access to content that is hosted on Google sites and ensures that policies aimed at student safety are consistently applied.

Innovation Hubs
Finally, Jamf announced the expansion of their MATTER Innovation Hub program, opening five new hubs within the last year. This program is designed to deliver state-of-the-art solar-powered Apple classrooms to under-resourced locations across town and across the world. Jamf and MATTER have now partnered to open a total of 14 MATTER Innovation Hubs currently impacting the lives of over 5,000 students.

For more information or to register for JNUC 2022, visit: https://www.jamf.com/events/jamf-nation-user-conference/2022/

About Jamf
Jamf's purpose is to simplify work by helping organizations manage and secure an Apple experience that end users love and organizations trust. Jamf is the only company in the world that provides a complete management and security solution for an Apple-first environment that is enterprise secure, consumer simple and protects personal privacy. To learn more, visit www.jamf.com.

Media Contact:
Liarna La Porta | media@jamf.com

Investor Contact:
Jennifer Gaumond | ir@jamf.com