Managing and Securing Apple Devices at Black Hat

By Adam Derrick, MDM Team Lead for the Black Hat NOC, and Victor Poh, Asia Sales Engineer at Jamf

One of my favorite things about supporting Black Hat is getting to take off my SE hat for a week. No customer calls, no demos, no Slack messages. Just actual hands-on work with the tools I spend the rest of the year talking about daily. In a lot of ways, I get to be the customer for once, and that perspective is something you can't get anywhere else.

If you've never been to Black Hat, the first thing you need to know is that it's an incredible event. Thousands of security researchers, hackers and IT professionals in one place, all sharing knowledge and pushing the industry forward. It's genuinely one of the best weeks of the year.

The second thing you need to know is that the network is absolutely hostile. Every person on it knows exactly what they're doing, and a fair number of them are actively looking for something interesting to find. That makes managing Apple devices at the event a completely different challenge from anything you'll face back at the office.

I'm Adam Derrick, a Solutions Engineer at Jamf and the MDM Team Lead for the Black Hat NOC. I've been an Apple admin for 20 years, with a focus on mobile and identity, and I've been supporting Black Hat for the past year. My colleague Victor Poh is Jamf's Asia Sales Engineer, supporting Black Hat alongside me and bringing 15 years of IT experience focused on mobile and security.

When 3,000 cybersecurity professionals descend on Singapore for Black Hat Asia, they're focused on the latest threats, vulnerabilities and defensive strategies. But behind the scenes, there's another critical operation running 24/7: a team securing the network, observing data movement within it, and managing the hundreds of Apple devices that power the event itself. Jamf is part of that team, bringing Apple device management and security to the devices every attendee and employee relies on.



Adam presenting at the NOC partner session

This is what we've learned.

The door most people walk past

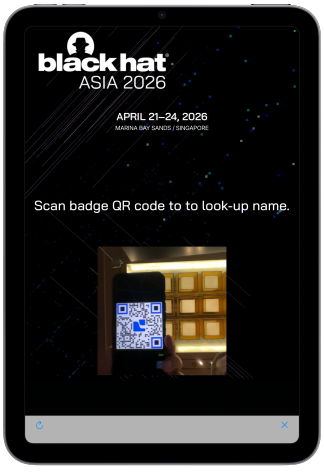


At every Black Hat conference there is a door that many attendees walk right past without a second thought. Step inside and you'll find the NOC in full operation: screens, telemetry, engineers, and a live view of one of the most complex event networks ever assembled. It's open to attendees, and it's worth stopping in.

So what exactly is the Black Hat NOC? The Black Hat Network Operations Center provides a high-security, high-availability network in one of the most demanding environments in the world. This is accomplished with the help of best-of-breed solution providers and seasoned security and engineering teams led by Black Hat's esteemed NOC team leads. Together, this team provides the security, stability and visibility of a world-class enterprise network. Each year, this hand-selected group meets months before the event to incorporate the latest infrastructure and security solutions into a workable network design, then reconvenes just days before Black Hat for a compressed deployment that must be fully operational by opening day. The Black Hat NOC program is a testament to engineering know-how and real teamwork. Behind every smooth conference experience, there's an extraordinary amount of invisible work holding it all together.

What Apple devices actually do at Black Hat

A lot of people think of Black Hat as a conference where you sit in sessions and look at slides, attend classes and learn ethical hacking. And yes, that's part of it. But there's a whole operational layer running underneath that most attendees never think about, and Apple devices are at the center of it.



Registration iPad devices are the first thing attendees interact with. You walk up, scan your QR code, your badge prints. That's it. From the moment an attendee approaches the kiosk to the moment they're walking away with their badge in hand, the average time is 20 seconds. That number only stays that low because the devices are managed, consistent and never asking anyone to troubleshoot them mid-queue. When you multiply that across thousands of attendees moving through registration at once, a single device going down creates a ripple effect fast.



Attendees utilize iPad devices managed and secured by Jamf to check in and retrieve their badges.

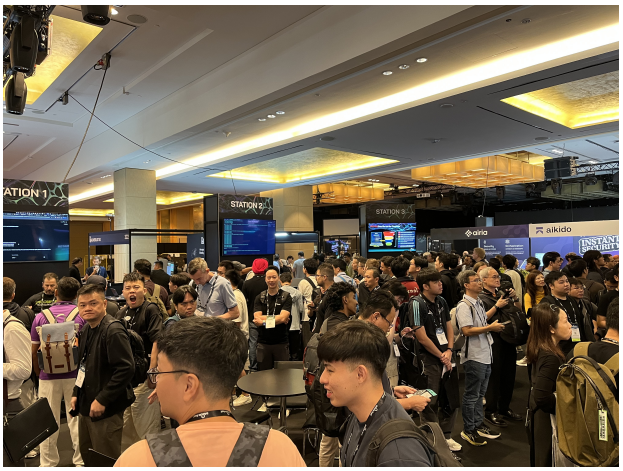


Session scanning iPad devices sit outside every training and session, tracking attendance throughout the conference. These devices move around constantly. They change hands between staff, go from room to room and need to work without any setup time when a session is about to start.

Lead scanning iPhone devices go into the business hall, where sponsors use them to scan badges and capture conversations with customers and prospects. These end up in the hands of sponsor staff who may have never touched a managed Apple device in their lives.

The scale adds up quickly. We're not talking about a handful of devices someone threw in a bag. This is a real fleet, and every device in it directly touches either the attendee experience or the business running the event. Keeping them available, consistent and secure isn't a nice-to-have. It's what the whole operation depends on.

Each role matters. Each one failing has a real impact on the people running the event and the attendees counting on it working.



Attendees in the Black Hat Arsenal attending sessions

Finding the friction that was worth fixing

Starting at Black Hat Europe 2025, Jamf was chosen as the official device management and security partner for the Black Hat Network Operations Center (NOC), managing and securing every Apple device powering the event, from backstage infrastructure to front-line operations. As a new partner, we found plenty of room for innovation.

Jessica Bair Oppenheimer, Director of Security Operations at Cisco, put it simply:

> *"Jamf was a clear choice to hand off this critical mission in securing the personal information of Black Hat conference attendees, staff and sponsors. The seamless integration that was already in place has been amplified and battle-tested in the environment of the Black Hat network."*

We were new to the game. But being new meant we came in with a fresh set of eyes, and what we observed got us thinking about innovative ways to address them.


Jessica Oppenheimer leading a training with the Cisco team in the NOC

Every device had a sticker on the back. Until it didn't. If you wanted to know what a device was supposed to do, you looked at the sticker on the back. It was functional, barely. Stickers fall off. They don't update when a device gets reassigned. In a fast-moving event environment, a physical sticker is a terrible source of truth. To make it worse, registration iPad devices are locked inside a kiosk, so that sticker was sitting underneath a key where nobody could read it anyway. What did work was having Autonomous Single App Mode in place, which locks devices into a secure kiosk state while still giving

our support team a clean way out: a simple gesture or passcode for troubleshooting, no full unlock required.

Tagging devices in MDM was completely manual. Getting hundreds of devices assigned to the right roles in the MDM system meant touching each one individually. It was slow, it was error-prone and when something got misconfigured, you usually found out at the worst possible moment.

Staging iOS devices took forever. The old approach meant walking through setup on each device by hand: screens, confirmations, configurations, one at a time. At Black Hat's scale, that was hours and hours of work before the event even opened. People were exhausted before things got started.

What we changed

Once we clearly saw the problems, the fixes became obvious. And Jamf had the tools to make all of them happen.

Jamf Mobile Assist replaced the stickers. Rather than a physical label, Jamf Mobile Assist deploys a virtual asset tag directly on the device, showing the device name and its assigned purpose (Registration, Session Scanning, Lead Scanning) right there on screen. No stickers. No mystery. The device tells you exactly what it is.



The device displays a virtual asset tag with the room location on both the home and lock screen, updated in real time without anyone touching the device.

Staff can change device roles in the field. Jamf Mobile Assist lets staff select a device's role directly on the device. The app is passcode-protected so random people can't mess with it, but the right people can reassign a device in seconds. At a busy event, an iPad might need to float from one room to another to cover a different session or support a different function entirely. With Jamf Mobile Assist, staff just pick up the device, select the new role and walk. No IT ticket, no call to the help desk, no one logging into the management console to push a new configuration. The device is ready before they reach the door.

Zero-touch enrollment changed everything. This was the biggest shift. We partnered with a device rental company that could provide Apple devices pre-enrolled in Apple Business Manager. Combined

with Jamf Prestage Enrollments and Return to Service to suppress Setup Assistant panes, staging went from hours of hands-on work per device down to a single tap. Devices come out of the box ready to go. The team shows up to the event ready to go. It's a completely different experience.

Black Hat is an incubator for innovation

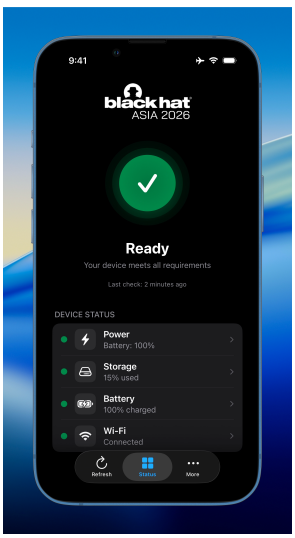
One of the things I've come to appreciate most about supporting Black Hat is that it doesn't just test what you've built. It shows you what still needs to be built.

Working the floor at Black Hat USA and Black Hat Europe 2025, I kept running into the same friction points. Jamf Mobile Assist was solving real problems, but there were gaps in how quickly staff could check the state of a device and act on what they found. I started thinking through what a purpose-built tool for that workflow would actually look like. That thinking turned into something real.

That feedback loop between field experience and product development is something Aaron Maxim, Senior Consulting Engineer at Jamf, knows well:

> *"Adam has provided us with valuable real-world feedback from Black Hat events. This has enabled the consulting engineering team to build applications like Jamf Device Checker and make improvements to other tools."*

Introducing Jamf Device Checker



Jamf Device Checker is built for the person holding the device, not the person behind the console. Available now on the App Store, it gives IT staff and end users an instant read on whether a device is ready to work. No technical background required. A clean, color-coded dashboard tells the story at a glance: green tiles mean you're good to go, yellow or red mean something needs attention. Behind that simplicity is real signal: iOS version compliance against company requirements, required app installation and update status, battery health and charge level, and storage availability with early warnings before space becomes a problem. Whether you're running a high-stakes event floor or just keeping a distributed workforce compliant, Jamf Device Checker puts the right information in the right hands without anyone needing to log into a management console to find it.

That's what makes Black Hat different from most places you'd go to talk about security tools. You're not just presenting ideas. You're stress-testing them in real time, in front of the people most qualified to find the holes. If something isn't working, you know immediately. And if you're paying attention, you leave with a much clearer picture of what to build next.

Jamf doesn't work alone at Black Hat

One thing that surprised me going into this was just how integrated the whole operation is. Jamf isn't the only official provider at Black Hat. We work alongside Cisco, Arista, Corelight and Palo Alto Networks to build and secure the network from the ground up. The NOC is where all of that comes together, and it gets stood up from scratch in about three days.



The Black Hat NOC team leads on stage for "Digital Infrastructure Decoded: NOC Partner Presentation" at Black Hat Asia 2026

One detail that stood out: roughly 90% of the partners staffing the NOC showed up with a corporate-issued MacBook. That might not sound remarkable on the surface, but historically NOCs and SOCs have been Windows-dominated environments. Seeing macOS that common in a room full of security professionals says something real about where Apple stands in enterprise today.

What Jamf brings to that table is mobile device management and iOS security. Cisco Security Connector runs on iOS devices at the event, providing security visibility and DNS protection at the device level, and Jamf manages the deployment of that software. So the same devices handling

registration and session scanning are also feeding telemetry into the broader security operation. At Black Hat Europe 2025, we also integrated Jamf Pro MDM with Cisco Duo Directory for Single Sign-On, a new addition that we're building on going forward.

Arista's role in that integration goes deeper than routing. Landon Harsh, Systems Engineer at Arista Networks, explained how the network layer and device management work together: "Jamf gives us complete control over which SSIDs our devices connect to. Registration runs on its own isolated network, and since Jamf deploys everything automatically, we never have to share keys. It just works."

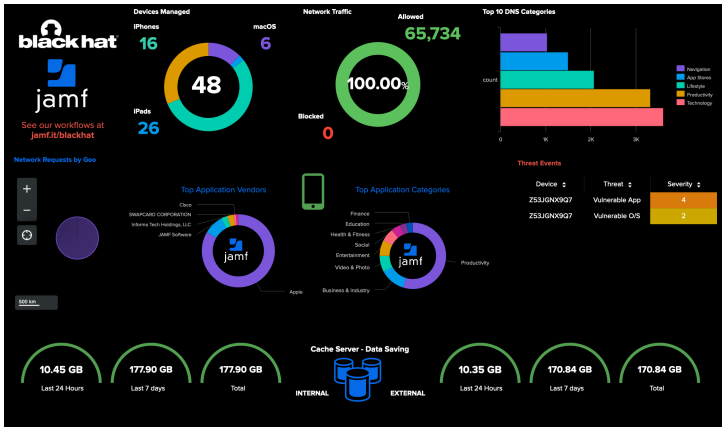
Something that often gets overlooked: at Black Hat, most devices on the network are personal. Attendees bring their own laptops, phones, everything. The managed iOS fleet is one of the only places at the entire conference where there's real endpoint governance. Jamf Pro gives us centralized configuration, policy enforcement and rapid remediation across all of those devices. When something needs to change on a thousand endpoints at once, it happens from one place. And when the NOC wants to know the state of the managed fleet, they don't have to guess.



Black Hat attendees anxiously await the opening of the business hall. Their personal devices are connected to the public WiFi provided by the Black Hat NOC.

How the security data flows

Jamf Security Cloud runs continuously across all managed devices, monitoring for threats in real time and streaming that data into Splunk. The NOC team isn't waiting for something to break. They have a live feed of device risk scores, app versioning status, and vulnerability data including CVE identifiers and CVSS scores. When something needs attention, they can triage by actual severity rather than guessing. That data flows through Jamf Security Cloud into Splunk, gets enriched in Cisco XDR with device context, ownership and posture, and surfaces where the team can act on it fast.



Splunk dashboard showing real-time data from Jamf Pro, Jamf Security Cloud, and Content Caching metrics.

Palo Alto Networks brings Cortex XSIAM into the mix, ingesting Jamf telemetry to build a fuller picture of the device landscape across the event. Rabin Bhattarai, Sr. Technical Product Engineer at Palo Alto Networks, explained what that looks like in practice: "Visibility is the foundation of modern security. By ingesting Jamf telemetry into Cortex XSIAM, we've gained a comprehensive look at our device inventory and check-in patterns. This data provides contextual baseline for the BH NOC to distinguish between routine device check-ins and genuine anomalies."

Jessica Oppenheimer is clear-eyed about what makes that dynamic work:

> *"It's essential to have continuity in the leadership of the NOC and SOC partners. Although the companies we represent sometimes compete for market share and mind share, in the Black Hat NOC there is a unified mission to ensure there are no gaps in our security posture. We build that together."*

What it feels like when it works

Victor also shared what the experience meant to him personally:

> *"I always wanted to attend Black Hat. I have heard many stories from friends and customers who have tried ethical hacking at the event. It is amazing to see the NOC comprised of partners that may be competitors who take off their company hat and all come together for a common purpose. I am honored and privileged that Adam and the NOC team invited me and I look forward to supporting future events!"*

After 20 years of Apple admin work, getting to apply all of it at Black Hat has been genuinely satisfying. The environment doesn't forgive sloppy processes. Either your setup holds or it doesn't. Getting to a place where it just holds, every time, is what we're both proud of.

One of the highlights of Black Hat Asia 2026 was getting to make that work visible. The NOC team leads delivered "Digital Infrastructure Decoded: NOC Partner Presentation" to a packed room, walking through how Arista, Cisco, Corelight, Jamf, MyRepublic and Palo Alto Networks each own a layer of the stack and how those layers fit together into something that's both reliable and genuinely secure. Most attendees walk right past the NOC. This was a chance to open the door and show what's actually inside. The questions from the audience were sharp, which at Black Hat is the best compliment you can get.



Adam Derrick speaking to a large audience at the "Digital Infrastructure Decoded: NOC Partner Presentation" session

What you can take from this

You don't have to be running Black Hat to face these challenges. Any time you're managing Apple devices at scale across an event, a large campus or a distributed team, you hit the same walls: devices need clear roles, people in the field need to make changes without calling IT, and nobody has time to stage hardware by hand.

What Black Hat makes clear is that Jamf is more than device management. Jamf Mobile Assist, Automated Device Enrollment, Return to Service and Jamf Device Checker cover the operational side: getting devices into the right state, keeping them there, and giving anyone on the floor the visibility to act without logging into a console. Jamf Security Cloud covers the security side: monitoring for threats in real time, feeding telemetry into the broader security stack, and giving the NOC the signal it needs to triage by actual severity. Application Insights rounds it out with app installation status, version compliance and usage data across the fleet. Together they cover the full lifecycle of a managed Apple device: deploy it, secure it, monitor it and support it. All of it is part of the Jamf platform, already available to Jamf customers. No extra integrations, no bolt-ons.

Recent security breaches have taught us something that doesn't get talked about enough: protecting your devices means nothing if your MDM console itself isn't protected. "Attackers aren't hacking in, they are logging in." Tools like Jamf Mobile Assist and infrastructure as code help address this directly. Moving common tasks onto the device and deploying configurations programmatically through the Jamf Pro API keeps the console out of the day-to-day critical path. Fewer logins, smaller attack surface.

And for the times when someone genuinely does need console access, that's where Cisco Duo comes in. We enforce device-bound authentication on both Jamf Pro and Jamf Security Cloud: Face ID, Touch ID, a passkey, or the Duo app. The person asking to manage hundreds of devices has to

prove they are who they say they are. That's what turns a compromised password from a catastrophe into a near miss.

Being invited to work in the Black Hat NOC has been one of the most rewarding experiences of my career. Thank you to all the NOC leadership and partners! See you all in Las Vegas for Black Hat USA this August.



The Black Hat Asia 2026 NOC Team

NOC partners

Black Hat's network and security infrastructure is built and secured by an elite group of official partners, each contributing specialized expertise to one of the most sophisticated event networks in the world.



Resources

Jamf Device Checker

App Store listing: jamf.it/checkerapp

Configuration guide: jamf.it/checker

Black Hat Network Operations Center

blackhat.com/asia-26/noc.html

Black Hat USA | August 1–6, Mandalay Bay / Las Vegas

blackhat.com/us-26/

Getting Started with Infrastructure as Code

jamf.it/terraform

Jamf Concepts

jamf.it/concepts

Black Hat NOC Live Twitch Stream

twitch.tv/blackhatnoc

Follow Adam on LinkedIn

linkedin.com/in/derrad

Adam Derrick is a Solutions Engineer at Jamf and the MDM Team Lead for the Black Hat NOC, with 20 years of Apple admin experience focused on mobile and identity. Victor Poh is Jamf's Asia Sales Engineer, supporting Black Hat alongside Adam, with 15 years of IT experience focused on mobile and security.