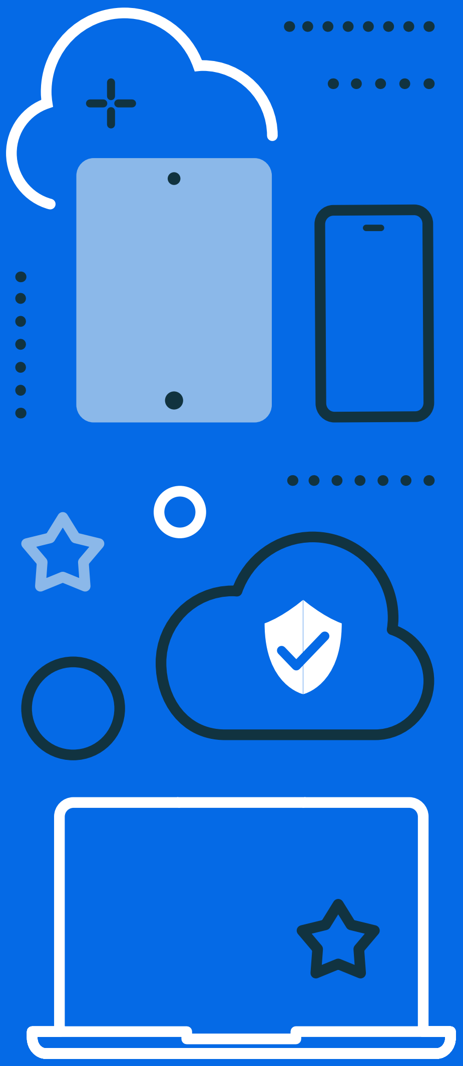


Data Policy and Management

for Beginners

jamf

Now more than ever, businesses are supporting remote and hybrid workers and they require more than just the basics of device management. Corporate mobile devices provide the freedom to work anytime, anywhere, but with this flexibility comes the drain of personal use and behavior on company devices, even on personally enabled devices on your cellular plan.

Jamf helps organizations enable and maintain remote work by ensuring that users remain productive, regardless of where users are located and what devices they're using as they shift to hybrid and remote environments.

By leveraging the following technologies, organizations can:

- Implement customizable policies to ensure compliance
- Configure data capping and alert thresholds
- Filter inappropriate content
- Extend policies to all network communications
- Monitor for and eliminate shadow IT
- Manage usage in real time

Learn what you need to know to establish an Acceptable Use policy and manage your company data and devices in a way that supports your company and end-user needs.

Managing devices is often seen as a very science-driven endeavor. Once backed by all sorts of data to arrive at the optimal management level to ensure devices, users, and data are protected and remain that way. And while that fact is not in dispute here, there is a bit of "magic" to being a successful administrator. Something that comes from experience and a thorough understanding of your network's unique needs. After all, despite the standards and best practices, each network is truly its own island operating under the specific policies of its organization.

"There's no such thing as magic!" *— Uncle Vernon*

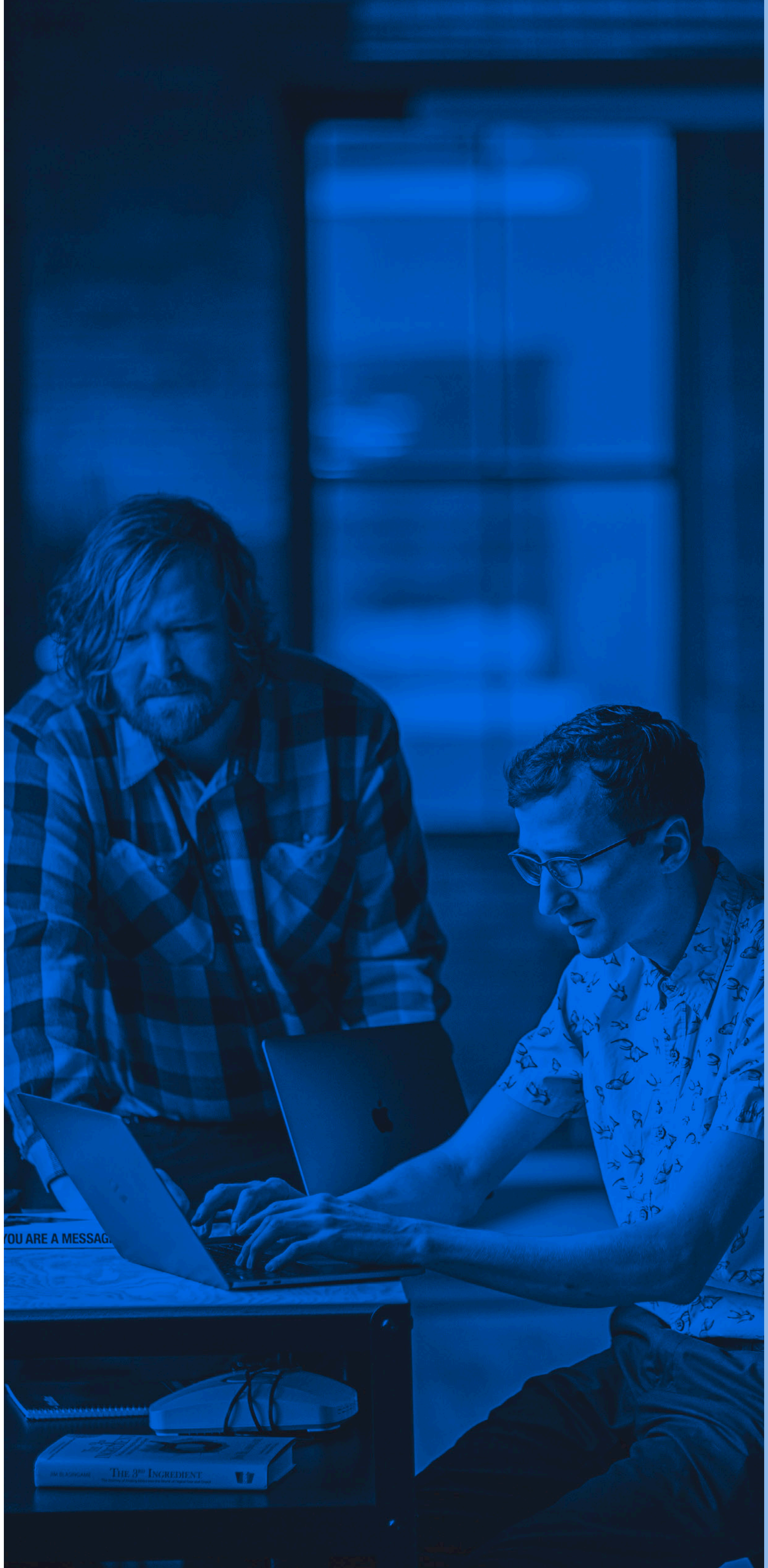
Doesn't it feel magical when your devices are performing optimally?

That data is secure, corporate applications and resources are accessible, yet protected. And users are happy, with the ability to use secured devices to perform work and personal tasks, without heavy-handed management practices preventing them from being productive or enjoying their downtime. How about when issues are detected, yet risk is mitigated through automation without IT having to lift a finger or the end user being negatively impacted?

That is the sort of magic that's wielded by Jamf admins. Going beyond the basics, Jamf Protect's data policy solution supports organizations in remote and hybrid work environments. Regardless of the device type or whether they are personal devices as part of a BYOD (bring your own device) initiative or a corporate-owned fleet is essential to have an Acceptable Use policy and place as well as the means to manage and enforce it.

Here's a starting point for creating or assessing your Acceptable Use policy. Consider how your organization can:

- Empower your admins to monitor data consumption with real-time analytics and granular reporting
- Enforce acceptable usage policies
- Eliminate shadow IT
- Filter content
- Implement customized protective policies to meet the needs of your users and organization
- Holistically support your network regardless of the device or ownership type

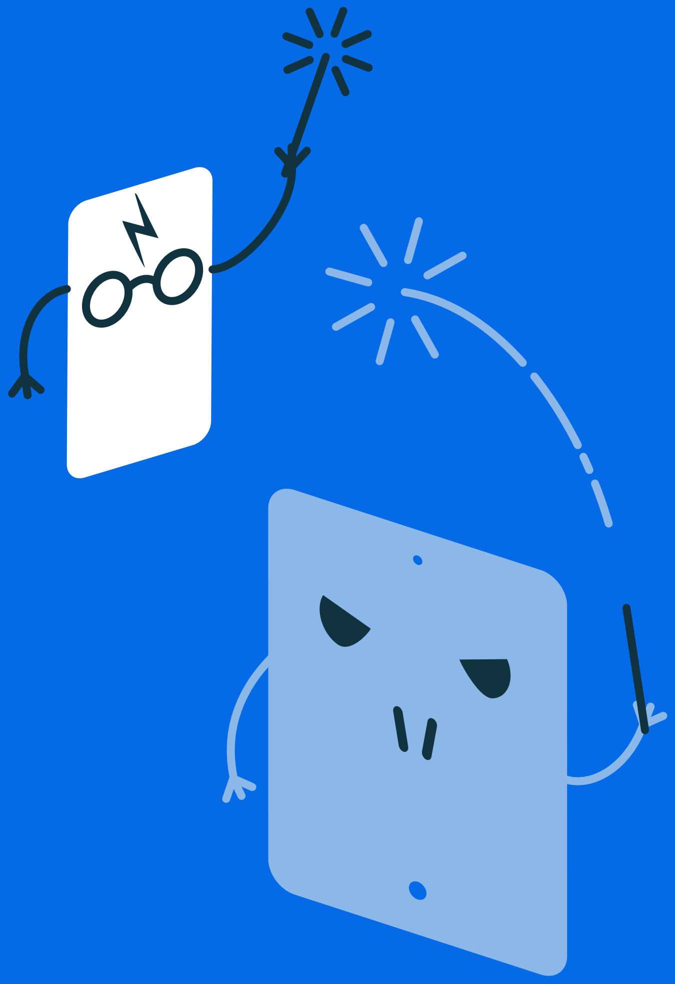


HARRY POTTER VS VOLDEMORT

Before diving into the data policy features of Jamf Protect, let's touch on some of the reasons why it's necessary to help your organization in managing the mobile fleet of devices on your network. And what better way to describe the use case than by invoking the greatest of the modern magicians, Harry....Potter, that's right!

In the series of books written by author J.K. Rowling, the wizards of the Pottermore universe share similarities with IT and security admins in that, they are presented with a choice: be like Voldemort or be like Harry — stay with us.

If you choose the way of Voldemort, your organization would rule with an iron fist, forcing users to adapt to your policies despite their needs or the unintended consequences.



But if you choose to fashion yourself after Harry, your organization would operate with fairness, opting to err on the side of compromise while working together to solve the greater problem.

“We must all face the choice between what is right and what is easy.”
– Albus Dumbledore

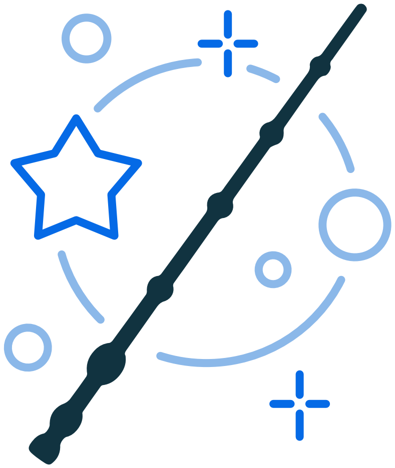
While it is easy for admins to choose the Voldemort path in the name of security and protecting users, the sad reality remains that often – the latter path presents more options to achieve data security and protect users since all stakeholders are working together to achieve this common goal and not fighting against excessive or restrictive controls that do little more than stifle productivity and ultimately alienate users.

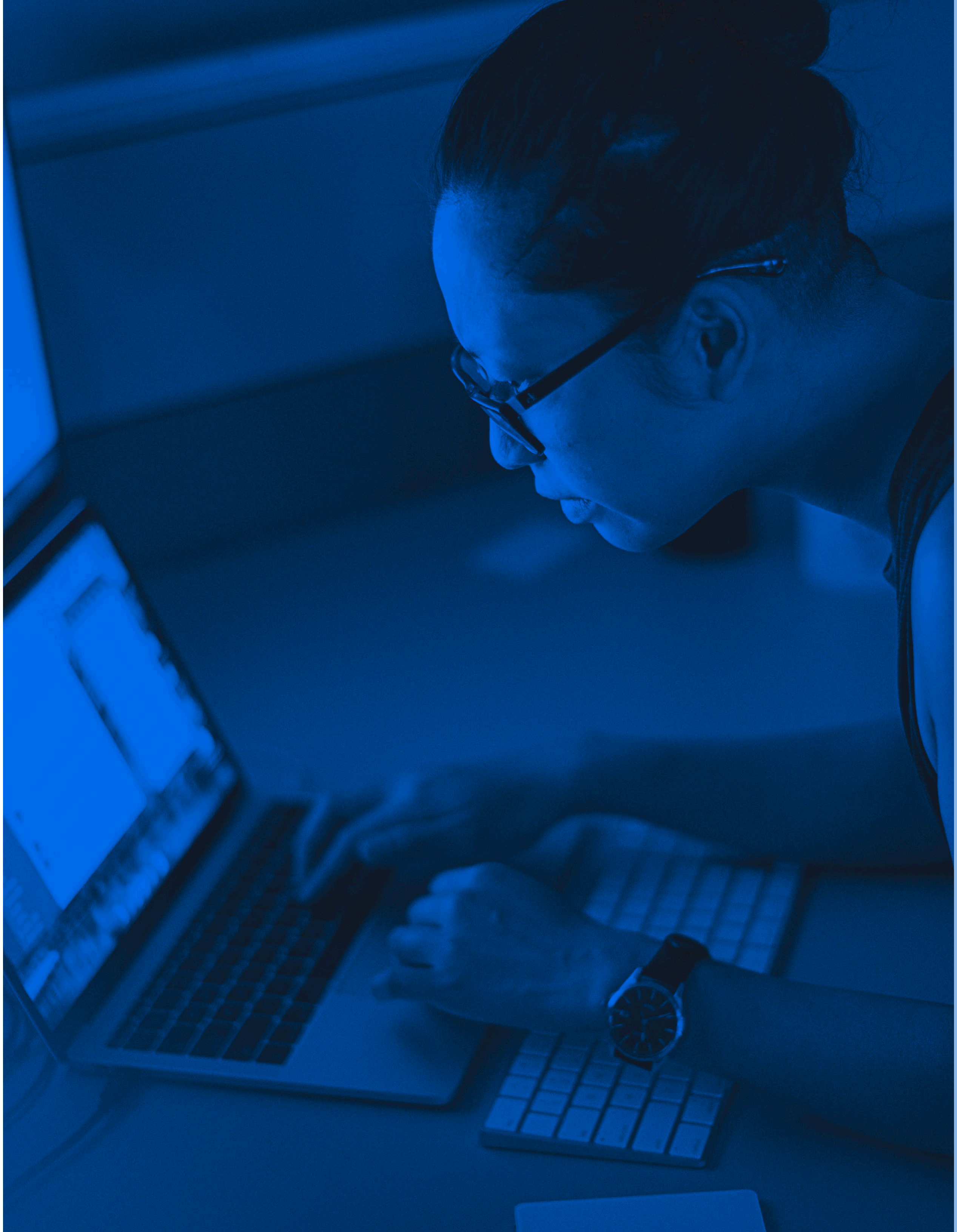
As mentioned earlier, every network is different and adheres to a different set of rules, policies, laws and regulations than the next. So when it comes to data policies and management, there is no “one-size-fits-all” answer. But with that in mind, administering devices in the Voldemort method will surely do nothing more than pigeonhole admins, effectively eliminating the fluidity necessary to monitor, detect, respond and remediate any potential issues encountered in the dynamic world of information technology. Wouldn’t you agree?

THE ELDER WAND

Like Harry Potter, IT and security admins are just people. Everyday regular people with skills that, while formidable, need a way to be channeled to be used effectively. Harry had the Elder Wand. You have Jamf.

Specifically, we'll drill down on two features that provide organizations the necessary defensive protections to comprehensively manage their mobile devices in a consistent and efficient manner.





REAL-TIME POLICY CONTROL

Configuring cap policies for data usage and applying them when thresholds are reached, defining which websites, services and apps can be accessed and providing visibility into usage with category-based controls – in addition to customizing them to trigger automation of policy enforcement — provide a glimpse into how organizational policies can be curated to restrict access to inappropriate content and apps that are not deemed business critical.

Over 50% of corporate data usage is not business critical, according to Jamf. This unprecedented level of visibility into data usage allows organizations to granularly configure data pools and network-based traffic use so that mobile devices are considered tools rather than objects that are to be abused due to lack of insight or controls.

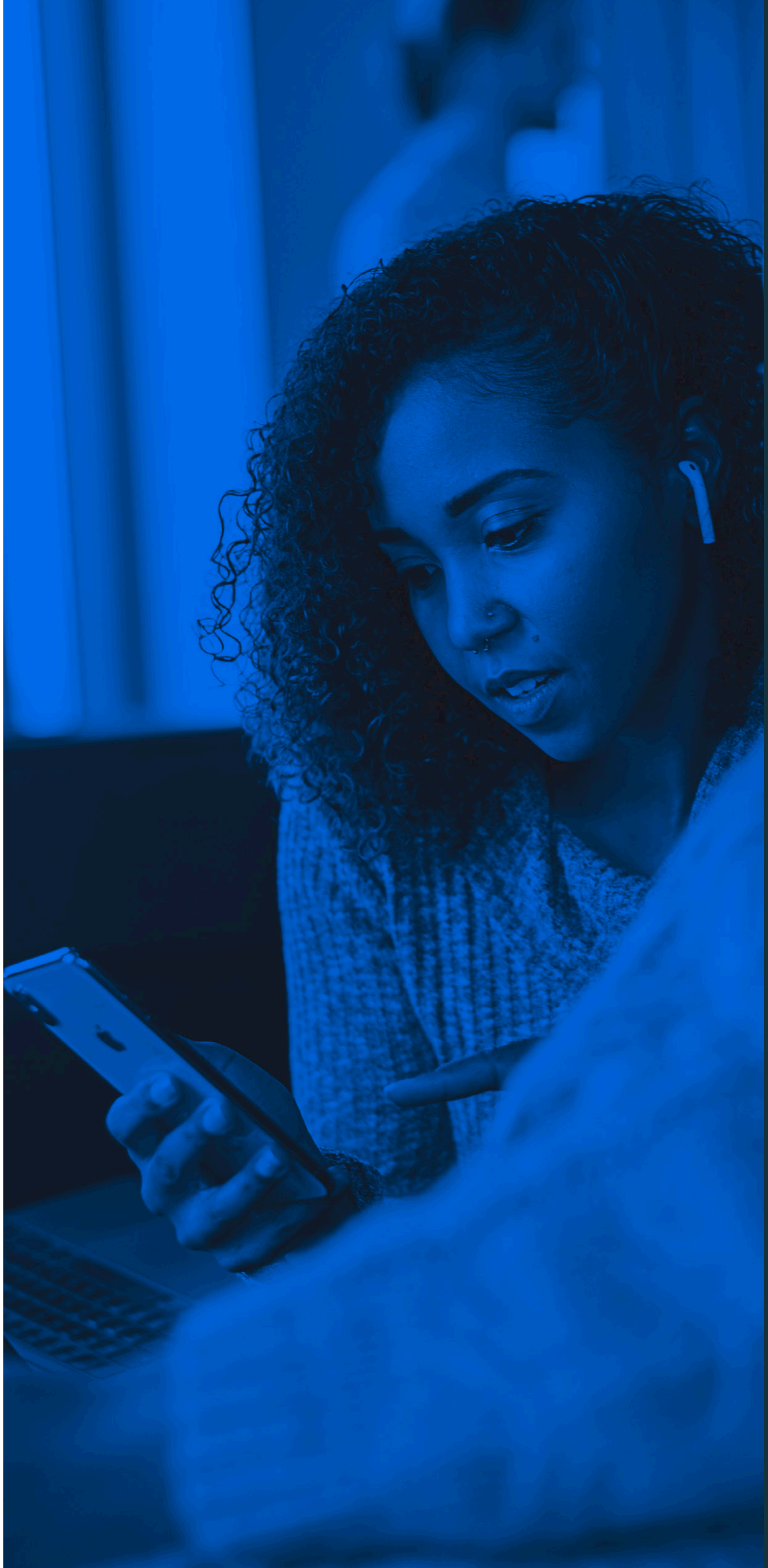
> ***"Time will not slow down when something unpleasant lies ahead."***
>
> *– Harry Potter and the Goblet of Fire*

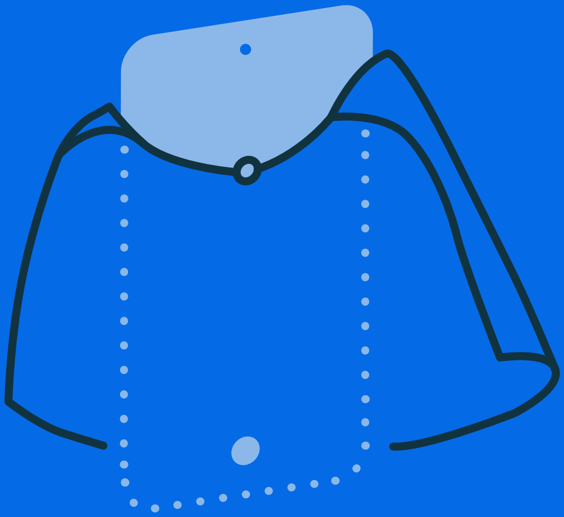
ANY MOBILE DEVICE, ANY OWNERSHIP MODEL

BYOD. CYOD. COPE. This bouillabaisse of acronyms all refers to mobile device programs that indicate varying degrees of support by program model. If figuring out which ownership model to support wasn't difficult enough on its own, the variety of different mobile device types, vendors and carriers will surely serve to complicate matters further, right?

Not for Jamf Protect, it won't.

The only decision your organization needs to make is choosing which devices are best for your business. Regardless of the device type, ownership model or operating system, Jamf supports the gamut of these choices, allowing admins to focus on managing mobile devices with the utmost attention devoted to security and compliance policies.





THE CLOAK OF INVISIBILITY

From an IT perspective, having a cloak that makes you invisible could be helpful when too many tickets are coming in at once. Imagine putting your head down and solely focusing on resolving issues instead of fielding wave after wave of emails, texts, calls and “quick questions”?

Well, if this speaks to you, there are a couple more features that might be of interest in helping to stem the tidal wave of requests through standardizing resource usage, enforcing compliance and setting user expectations.

FULLY CUSTOMIZABLE

No two networks are the same, and no two organizations will manage their requirements or infrastructure in the same manner. Largely, differences depend on the organization’s risk appetite. And similar to how enterprises modify their security posture to address risk, Jamf allows for full customization of policies and how they’re implemented for management.

From tailoring content filtering categories to customizing allow and block lists, policies can be applied holistically (the organization as a whole) to granularly, applying to a single user — or through group membership — the choices are flexible and work to address the needs of your organization. And most importantly, the choice is yours to make.

CONTENT FILTERING

Adult and gambling apps and services are significantly more likely to rely on unencrypted connections that may potentially expose organizations to risk through data leaks and compliance with regulatory bodies. Moving beyond the noted categories above, accessing content that contains weapons, hate speech or other forms of inflammatory materials may pose real civil and/or criminal consequences for users and/or the organization.

Not to mention the security threats that come from web-based content, such as phishing websites and other forms of malware that make their home across the four corners of the vast internet. Content filtering isn't solely about keeping the bad stuff out. If used proactively, it can be about only permitting the authorized data in by ensuring that acceptable websites, services and apps are reachable.

Furthermore, it is essential to reduce exposure to litigation by managing and maintaining compliant data usage and monitoring for and blocking access to unsanctioned services. Services like shadow IT can work to undermine the security posture of your devices and your network by inadvertently exposing sensitive corporate data.

THE PHILOSOPHER'S STONE

This section won't discuss the formula to brew the elixir of life nor how to turn common metals into gold, sadly, but it will discuss the next best thing: two more Jamf Protect features that — in their own way — perform their own bit of magic. By gathering real-time insights, IT and security admins can turn that data into actionable tasks used to better adapt to and manage their fleet.

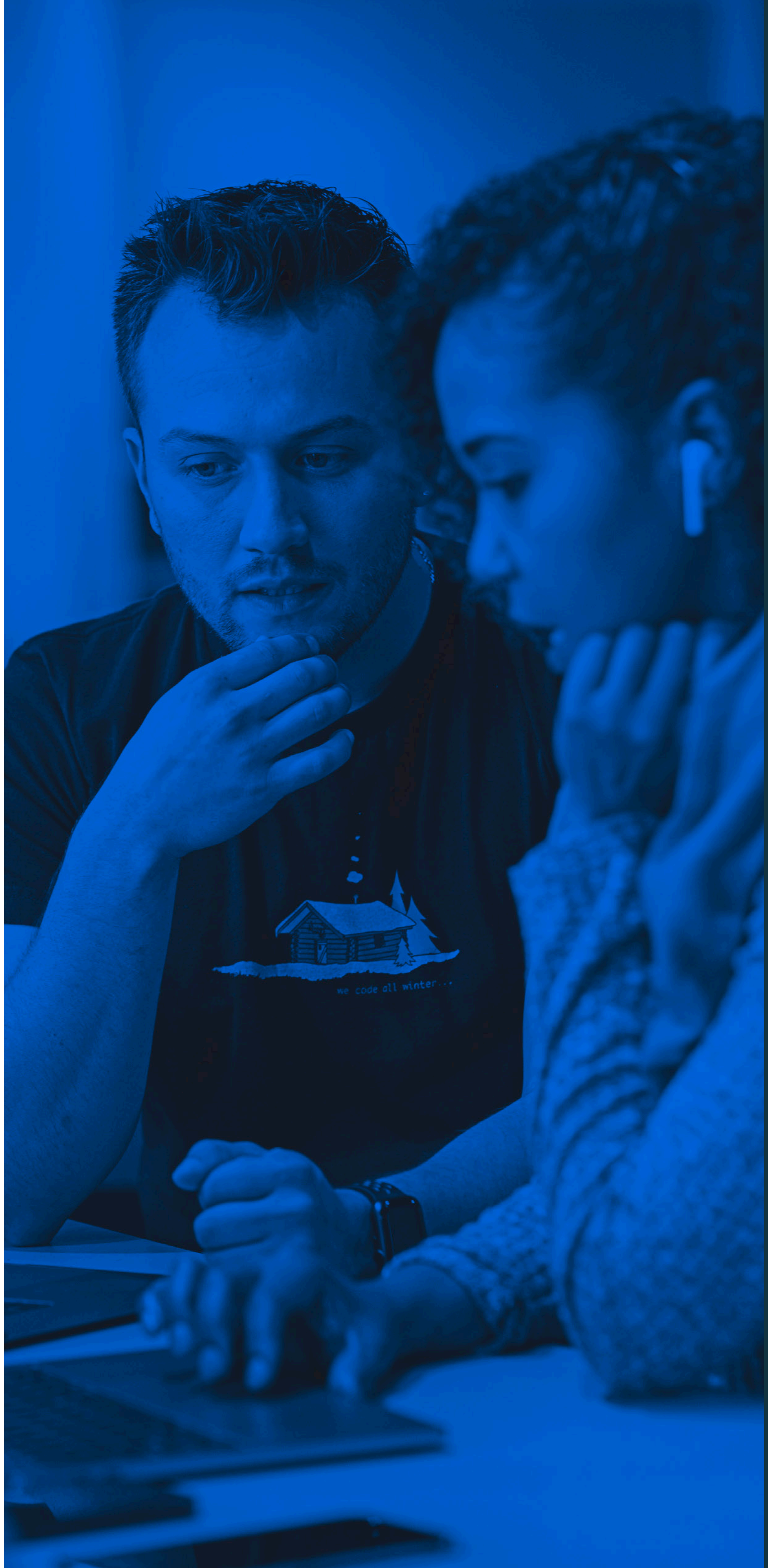
Going even further, the features make protections network aware, meaning that regardless of whether new sessions are spawned, or existing connections are closed, your devices and users will remain protected and compliant across all network connection types.

NETWORK AWARE

As we've established, one size most definitely does not fit all. Nothing embraces this concept more than the network connections on your mobile device. For example, when users are required to utilize metered cellular connections, they will often be more cognizant of usage limits due to additional charges they may incur from roaming and/or overage fees. However, if they can connect to a public Wi-Fi hotspot, chances are great that bandwidth concerns will not be a concern.

Jamf Protect clears up managing these murky waters by allowing admins to create and enforce policies for different network connection types and their unique variables.

Say your organization supports the COPE (corporate-owned, personally enabled) model and provides mobile devices to your employees for both work and personal use, however the cellular data plan is part of a data pool that's shared by all users. Your organization may want to restrict the bandwidth utilized by users so there's enough data to go around for everyone while on cellular, without instituting bandwidth management on Wi-Fi connections. Jamf Protect allows policies that can be implemented to do just that: limit bandwidth while on cellular but not Wi-Fi. Furthermore, the policies are smart enough to detect which connection is currently in use and adjust automatically without additional input from admins or impacting the end-user's experience.



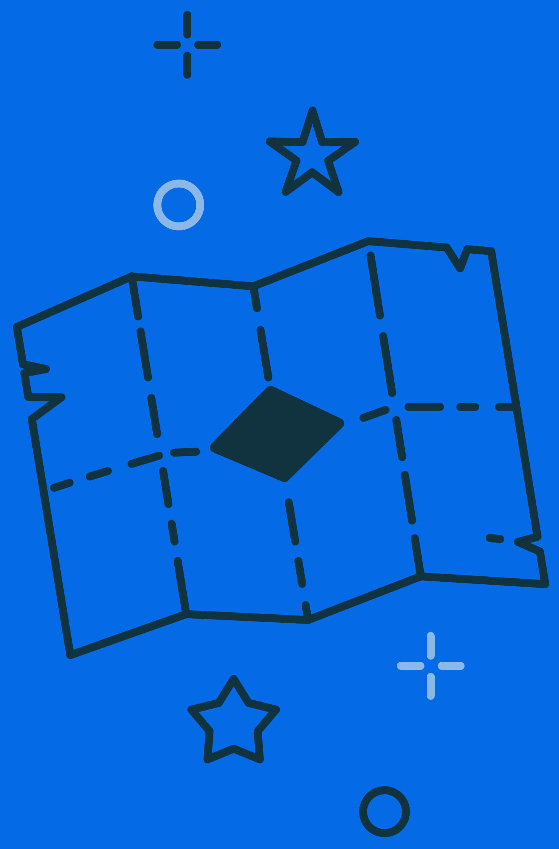
REAL-TIME INSIGHTS

"I solemnly swear I am up to no good." *— Harry Potter*

Ask any admin if they'd prefer to know when something is going to break or outright fail before it occurs (proactive) or after it does (reactive), and the answer will likely always be the same: they want to know beforehand.

Given the option, anyone would want to have a heads-up notice. If not to attempt to curb the event from happening, then to at least mitigate it as quickly as possible.

Huzzah! Jamf's real-time insights provide just that: preemptive notice through granular reporting that provides IT transparency over how devices are using their data and over which connections. Admins can proactively modify policies that may need to be more (or less) restrictive, make changes to existing data pools, configure content filtering to enable/disable access to certain apps and services, or simply just keep a watchful eye over a device's security posture.



NOW BOARDING ON PLATFORM 9¾

Having your mobile device fleet or users' personal devices enrolled in Jamf Pro is an excellent foundation for device management. But in today's modern work environments that center around hybrid or remote work, simply managing the physical device requires a more specialized tool.

With Jamf, you can:

- Manage how data is sent and received on the device itself through smart policies that are network aware
- Adhere to compliance regulations over any network connection
- Filter content with seventy intelligently designed templates to prevent devices from connecting to vulnerable, compromise and malicious websites, apps and services in addition to unapproved content

Lastly, data policy and management with Jamf Protect makes the job of IT and security admins simpler by eliminating shadow IT and enforcing acceptable usage policies for all devices – regardless of ownership level – to not only secure but also devices and users without disrupting the experience for stakeholders.

Request Trial

Get started today with a free trial, or contact your preferred reseller.