HEALTHCARE SECURITY

FOR BEGINNERS

Healthcare is like many organizations around the world that rely on technology to augment their business practices. As they occur, advancements drive – at least in part – how business continuity will proceed, often changing how things are done, stored and managed — or all three!

It's no secret that while the world at large has been rocked by COVID-19 and its variants, healthcare continues to get battered by its effects, both directly by the number of patients requiring care and indirectly by several related yet outside influences, like:

- Ongoing management of patient privacy data and records, users and endpoints while staying compliant with regulatory requirements
- Implementing changes to core business operations, like implementing telehealth, while balancing patient-caregiver safety
- Maintaining data security across all business models and protecting against threats and attacks from malicious actors, which are on the rise

“THREE IS THE MAGIC NUMBER”

There are many individual components that go into modern security practices. This e-book is not a guide to each and every piece of hardware and software out there but rather to understand the unique needs of the healthcare industry and identify the tools and processes that best address these needs.

Let's begin by looking at healthcare security with a high-level view of what buckets the components, tools and best practices fall into:

HARDWARE	SOFTWARE	COMPLIANCE

Resolving healthcare’s security needs isn’t as simple as picking a solution from each category. If it were that easy, security issues in general would not exist. These categories represent how solutions will apply to certain issues, some better than others.

For example, Jamf Protect monitors, detects, prevents, remediates and reports on malware-related incidents on your Mac. Malware largely targets software and requires a software-based solution to protect against, so endpoint protection would fall into the software bucket.

Hardware

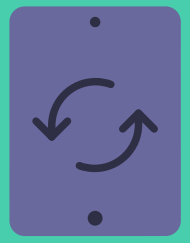
Threats and attacks that target your Apple devices directly fall under the hardware category. Security practices that aim to shore up vulnerabilities which would otherwise grant physical access to devices — like full-disk encryption to protect data-at-rest, enabling startup passwords to prevent unauthorized access to the boot menu on macOS or unlocking your iOS device — also falls under this category.

Software

When considering what falls into the software bucket, make sure to consider threats and attacks that primarily target and/or operate within the operating system itself.

Category examples:

- Endpoint protection
- Requiring VPN (virtual private network) or ZTNA (zero touch network access)
- App lifecycle and patch management



Compliance

Compliance is arguably the most important category in this trinity, and is also the one wrought with the greatest level of concern from all stakeholders. Compliance does not discriminate between hardware or software solutions. Stakeholders within the compliance category are mostly concerned with auditing, achieving and maintaining compliance with **regulations that govern healthcare practices**, like the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**.

There are myriad ways to support **compliance management**, but there are great starting points for any team:

- Security information and event managament (SIEM) solutions that centrally manage logs
- Security monitoring tools that actively monitor device health and compare it against common security frameworks

Best practice tip:

Organizations should use security management frameworks like the **National Institute of Standards and Technology (NIST) SP 800-53 series** and/or **Center for Internet Security (CIS) Benchmarks** to ensure endpoints are hardened and organizations are following industry best practices.

“OUR TRUE ENEMY HAS YET TO REVEAL HIMSELF.”

– Michael Corleone

Much like the character portrayed by Al Pacino in The Godfather, Part III who faced down a number of enemies – known and unknown – information security similarly battles against a seemingly never-ending horde of malicious threat actors.

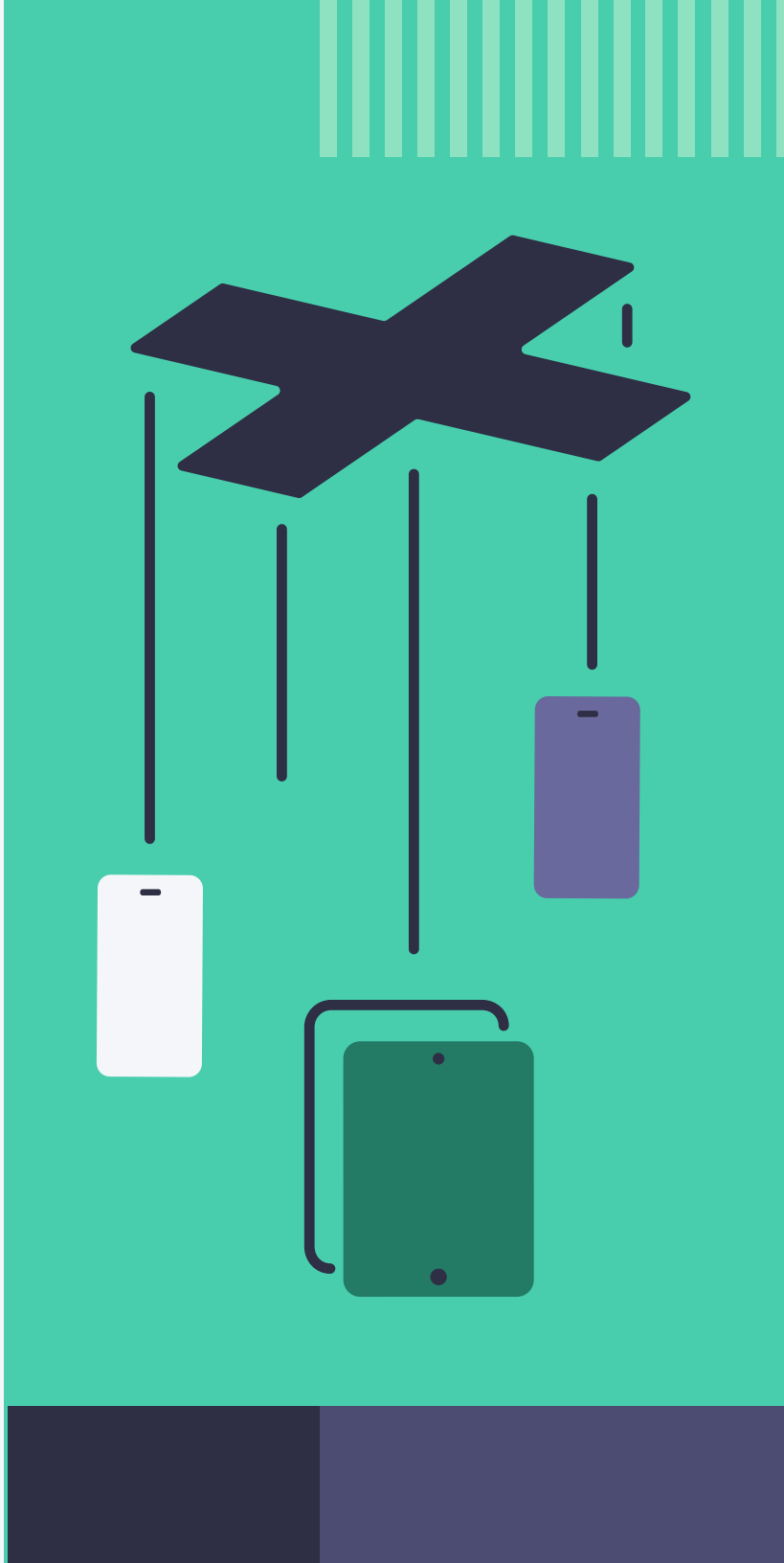
While the attackers themselves may be “faceless”, the threats they utilize to attack and compromise endpoints are known. Armed with this information, healthcare IT and security administrators can best protect their devices by:

- **hardening** device settings
- **managing** devices
- **implementing** endpoint protection
- **maintaining** devices with up-to-date patches
- **monitoring** devices in real time
- **triaging** detected issues
- **remediating** risks

AND

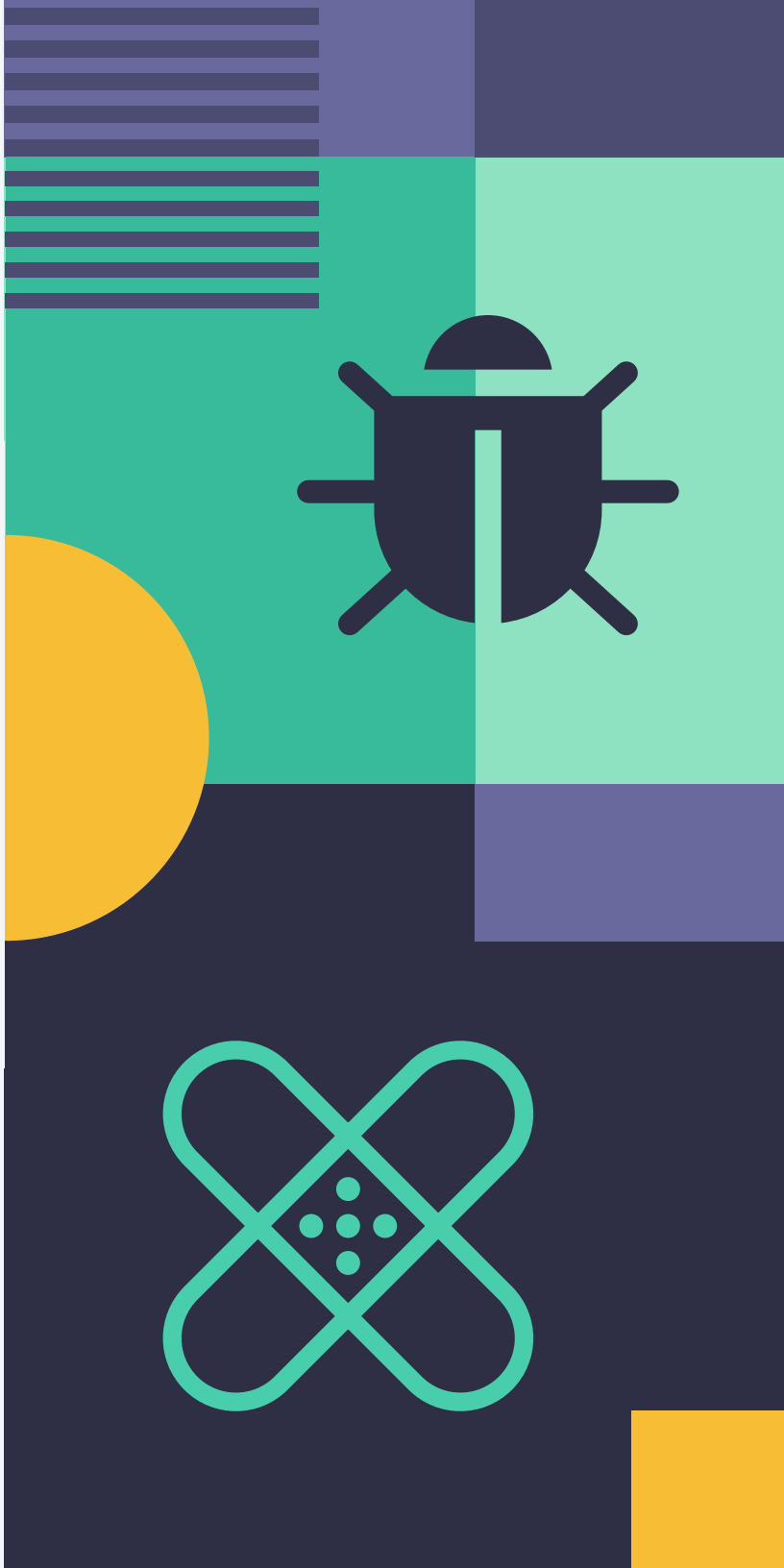
- **maintaining** device compliance...

...to protect all stakeholders from device compromise, data loss/theft, security breaches and events that would otherwise negatively impact performance, the end-user experience and the level of care provided to patients.



Among the potential threats, the following list represents concerns that are specific to healthcare providers:

- Malware-based attacks — like ransomware and denial of service (DoS) — can cripple systems and prevent providers from being able to use equipment to administer mission-critical, life-saving aid.
- Devices that are not up to date or current on patches and system/app updates leave organizations open to known vulnerabilities for subsequent exploits that can result in data breaches, leaks and/or theft of Personally Identifiable Information (PII) or privacy-regulated records.
- Providers rely on the technology they use to meet a minimum level of usability. Time spent and minutes wasted on devices that are not functioning properly — be it due to missing functionality or apps not updated — have real consequences. A device that is configured for an employee in the HR department will be of little to no real-world use for a doctor making their rounds, and vice-versa.
- Government regulations provide guidance as to how privacy and health data should be collected, stored, managed, shared and disposed of. Any data leak has the potential to incur regulatory oversight resulting in civil and/or criminal penalties, not to mention the possible loss of patients or facility closure due to damaged reputations.



“THE GREATEST VICTORY IS THAT WHICH REQUIRES NO BATTLE.” — Sun Tzu

The issues that pertain to healthcare security and managing them effectively are varied. They are not limited to a singular deployment manner. Malicious actors employ multiple methods to achieve their goal of bypassing an organization's defenses and compromising their target.

The good news? Healthcare security should not be singularly deployed either. In fact, the strategy of “defense in depth” is the best approach for mitigating the multiplicity of threats. By layering several defensive protections in a concerted effort to thwart attacks, organizations can identify security failings and deploy remediation workflows to resolve them and minimize risk.

Endpoint protection

Protection against malware is considered by many to be the most critical piece in any security blueprint to safeguard devices, users and data. And while that line of thinking isn’t entirely unfounded given the capabilities of **endpoint protection** software, like **Jamf Protect**, to prevent known and emerging threats across your entire fleet of macOS devices, the reality is that is one variable in your organization’s overall security posture.

Protecting devices against malware threats plays a significant role toward reducing risk, securing data and minimizing downtime for your end users. There are many endpoint protection software options available, but there are specific the features that healthcare providers will certainly want to look for are:

- Active monitoring for real-time threats
- Signature and analytics-based detection of known and potential threats
- Prevention of known malware to eliminate threats
- Remediation of identified threats and malware
- Alerting system that notifies the end user of threats detected/remediated
- Real-time reporting that provides Mac admins multiple levels of insight, from high-level summaries to granular details
- Low resource footprint for agents installed on endpoints: less resource utilization = better performance

There are capabilities that are not necessarily required but certainly make life easier for IT and Security teams, while bolstering the ability to respond to, triage and remediate issues found:

1. Integration capabilities with other products. For example: communicating device health findings from your endpoint protection with your MDM solution to **enable Security Orchestration, Automation and Response (SOAR) workflows that automatically remediate issues detected**, like removing malware and performing clean up tasks.

2. Especially important in highly regulated environments, **alignment with security frameworks** that provide industry-approved guidance based on best practices for configuring devices and measuring the key metrics that support the highest level of security possible.

Device management

Leveraging a mobile device management (MDM) suite is the key to effective, efficient and proactive management of your fleet of macOS and iOS devices. While there's nothing stopping IT from utilizing Apple's native configuration tool, Apple Configurator 2, to configure each device manually, the reality of this process is that the app was designed to handle only a few devices at a time. Anything more than that, such as when deploying and managing hundreds or thousands of devices, makes device management via MDM software – like **Jamf Pro** or **Jamf Now** – the clear choice.

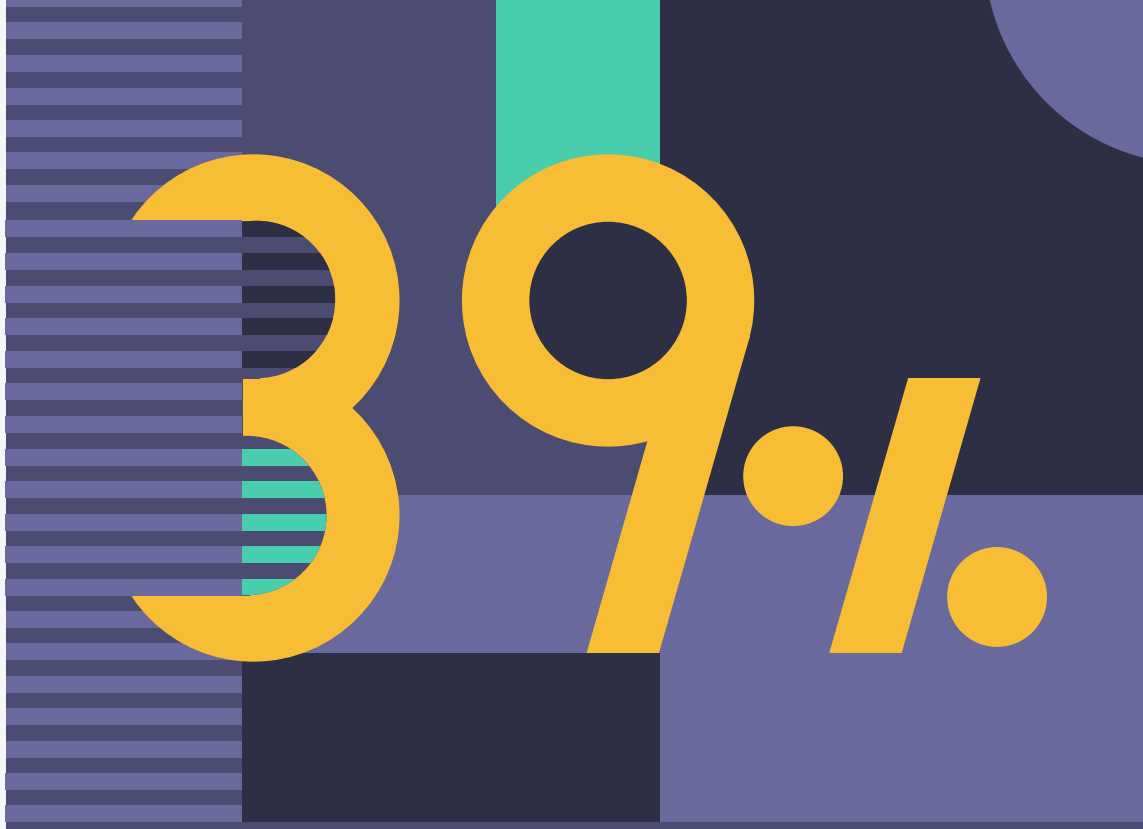
By aligning with Apple's management, security and privacy frameworks, Jamf Pro allows IT to manage entire fleets from a single, user-friendly dashboard, marrying advanced functionality with powerful workflows to keep devices configured and aligned with organizational policies without sacrificing the Apple end-user experience.

Device management enhances overall security by enabling organizations to:

- Simplify onboarding/offboarding by standardizing device enrollments
- Standardize configurations that act as templates to address needs common to certain departments, user types or groups — like all doctors having the same apps when documenting patient consultations or access to departmental peripherals, such as printers and scanners
- Develop policies that enforce organizational policies, such as an acceptable use policy (AUP)
- Deploy software and updates to devices and curate Self Service to display pre-authorized apps for users to install. No fumbling with Apple ID's or individual subscription costs/per user app fees
- Manage your inventory, including hardware, software and health statuses of your Apple fleet
- Implement modern identity management processes to track what devices are assigned to which users, including serial numbers, warranty information and servicing status
- Track and locate missing devices in real time while minimizing data loss risks with remote lock and wipe commands

App lifecycle management and patch support

How does your organization perform operating system and application update cycles? Are updates tested in non-production environments for compatibility prior being deployed on production systems? Moreover, what system of checks and balances are in place to verify that devices in your fleet are up to date on patches? If the response to any of those questions is "?" then your organization may be a part of the 39%.



What is the 39%, you ask? That's an excellent question!

The 39% refers to the percentage of organizations that, according to key findings published in Jamf's **Security 360: Annual Trend Report**, **"allowed devices with known OS vulnerabilities to operate in a production environment with no restrictions to privileges or data access."**

This is problematic since a significant number of **Common Vulnerabilities and Exposures** (CVE) rely on unpatched vulnerabilities to attack and compromise endpoints. The CVE's list of publicly disclosed cybersecurity vulnerabilities is maintained by the **MITRE Corporation** and is sponsored by the U.S. Department of Homeland Security (DHS) and **Cybersecurity and Infrastructure Security Agency** (CISA) with over 160,000 unique CVE records that vary in severity.

Again, its essential to have an MDM solution that provides versioning levels for installed software on your device fleet and app lifecycle management capabilities that allow IT to:

- Determine which devices require updates to operating systems, applications and peripherals
- Identify which patches are required when compared to an updated listed of current patch versions
- Disable apps and services that do not have patches available or are no longer supported by the developer and pose a threat
- Use Jamf's "Smart Groups" in conjunction with "Policies" to efficiently provide updates to the devices, and only those, that require them

Hardening devices

Securing devices is by no means a trivial task. Depending on your environment, organizational needs, regulatory requirements and number and types of devices to configure, the process could take a few minutes to several hours per device to initially configure. Typically, the larger the fleet the greater complexity between user types/ departments and compliance requirements. So naturally, the larger the fleet the longer it will take IT to get devices hardened. After all, securing one hundred devices within one department will take far less time than configuring fifty devices across five different departments, with half that number located off-site.

This highlights the importance of procuring the right tools for the job. In this case, hardening presents a “locking down” of features that are either unnecessary or need to be configured for a specific purpose to align with organizational policies. It also serves the purpose of limiting the attack surface of devices to provide **fewer attack vectors for malicious actors to gain access**.

A large majority of these features are configurable using the MDM solution used to manage your fleet. The key to maximum macOS and iOS support is to ensure that your solution provides **same-day support** for the latest Apple operating system releases which includes supporting Apple’s device management, security and privacy frameworks. This provides comprehensive support for:

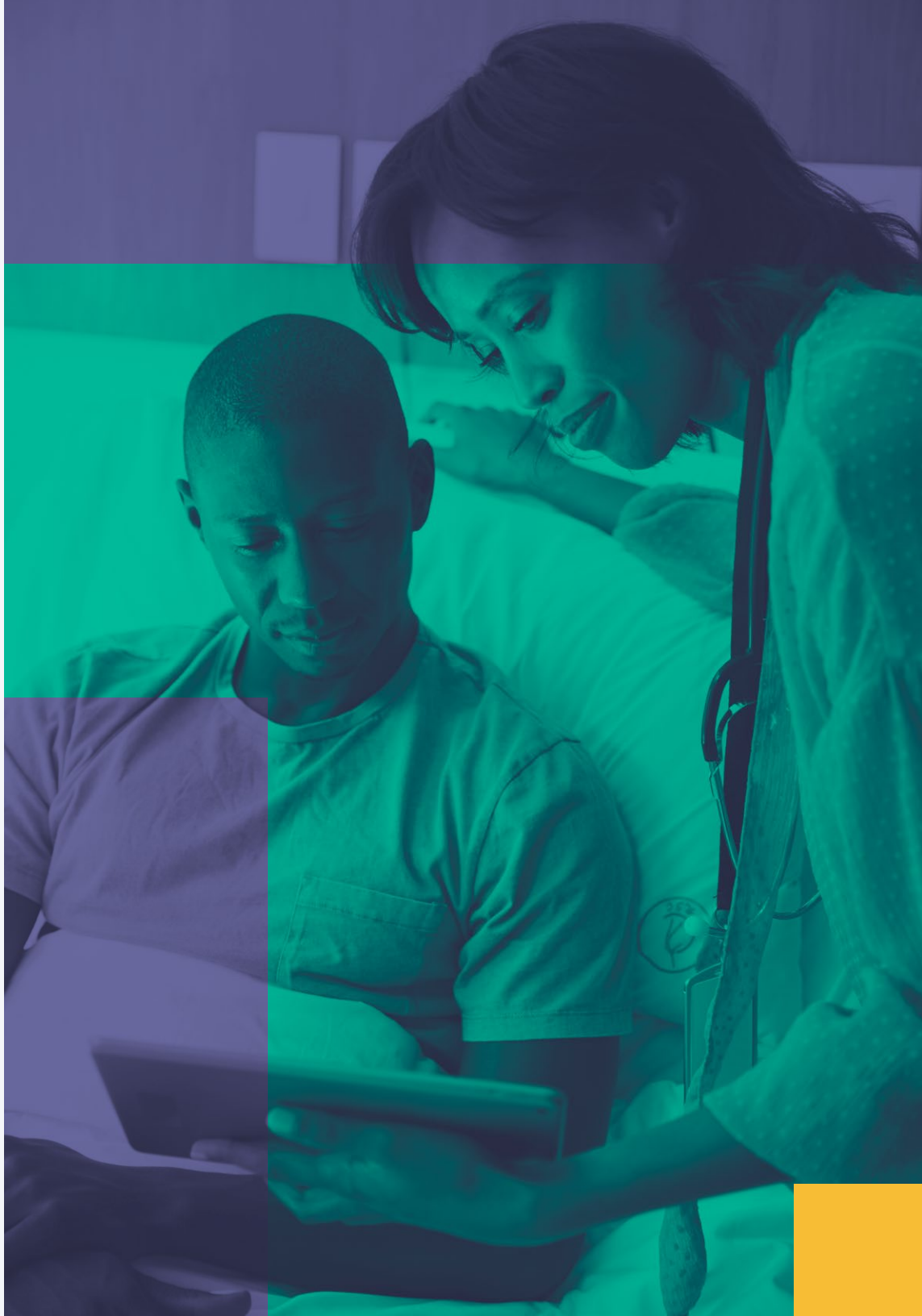
- Commands used to manage devices
- Configurable settings to further secure devices
- Adherence by all apps to user privacy controls

For example, enabling FileVault’s full-disk encryption is necessary to protect data at rest from unauthorized users and, in the event of a device becoming lost or stolen, it ensures that private data stored on the device is unreadable to anyone without the decryption key. Without the proper support, however, even users with valid accounts may not be able to unlock the drive’s contents if their account is not added to the FileVault user’s security group for that device. When your **MDM solution administers FileVault correctly**, it adds the user to the appropriate group so users can access the secured data. And in case of emergency, a recovery key is automatically generated and stored in the device record within the MDM for retrieval.

Secure access and communication

We've covered the importance of endpoint protection, managing and hardening devices and keeping devices up to date. Now, transition to securing network connections with **solutions made with modern computing in mind**, and how that plays a crucial role in keeping data safe, maintaining its integrity, and protecting it against unauthorized threat actors without impacting end users.

Five to ten years ago, VPN was your primary method for securing communications, that would have been a reasonable approach. VPN was — and for some may still be — the de facto standard for encrypting network connections, especially when accounting for remote connections to organizational resources. But in modern remote/hybrid work environments, like telehealth, the VPN model of security is outdated and simply does not offer **the flexibility and added security and access protections** that ZTNA does.



According to **Gartner**, ZTNA is a product or service that creates **an identity- and context-based, logical access boundary around an application or set of applications**. In a nutshell, the security model creates application-based microtunnels. Because of this, stakeholders can rely on the same benefits:

- Only authorized users can connect to healthcare applications
- Policy enforcement is consistent across all resources and clouds
- Microtunnels enforce least privilege access and prevent lateral movement
- Enable single sign-on (SSO) authentication for unified authentication across all devices

VPN does get some things right but at the cost of a few considerable security issues, like its reliance on providing users access to all resources when VPN access is granted – not just what the user specifically needs. Another big issue, and one that is completely out of IT's hands to manage, is that users must elect to connect to VPN before any protections to safeguard data are enabled. This is evidenced in **a survey conducted by security.org** where the question was asked, "Do you use a VPN?" to which 43% of users replied with, "I know what it is, but I don't use one."

Behind the scenes, **ZTNA ensures that the user is authenticated, authorized and that the device can be trusted to access the data directly**.

Identity provisioning

How you **manage user identities and provision access** to company resources is essential to managing security in any environment. When it comes to healthcare security and compliance, it is absolutely crucial to get it right. From the critical work of caregivers to the regulatory requirements dictating data policies, access and usage, there is little wiggle room for time — and even less room for error.

So, why manage user accounts manually or ad hoc when this method relies heavily on manual intervention, making it so prone to human error? You shouldn't; it is neither efficient nor effective. In dynamic, fast-moving environments, organizations benefit from standardizing account and access provisioning to automate workflows. With proper identity provisioning standards and workflows, end users have secure access to what they need, when they need it, and from any device, anywhere.

Leveraging cloud-based Identity Providers (IdP), alongside single sign-on (SSO) technology allows IT to create automated workflows that act as templates to:

- Standardize onboarding new employees
- Streamline hardware deployments
- Provisioning access to resources, including apps and services
- Implement and enforce password policies
- Synchronize passwords across all device types
- Integrate with ZTNA to limit access to resources when access is compromised without preventing access to unaffected services

Deploying hardware

While deploying new devices, such as MacBook Pro laptops and mobile devices like iPad or iPhone, would appear on the surface to be a simple matter of: purchase devices, configure devices and deploy devices. However, there are often obstacles or hang-ups to parts of this process. Whether they are procurement issues or those related to coordinating the logistics behind getting the devices into the hands of the users, chances are pretty great that the biggest hurdle (timewise) will be provisioning process.

But that doesn't have to be the case. As a matter of fact, Apple has gone to great lengths to make sure their devices can be deployed with almost no hands on the devices via zero-touch deployment. IT can deploy devices with ease utilizing the zero-touch model in no time flat:

- ☑ Sign-up for an Apple Business/School Manager account
- ☑ Link your Apple Business/School Manager account to your MDM solution
- ☑ Configure Pre-Stage Enrollment Profile settings

That's it!

As your organization purchases equipment from Apple (or it's authorized resellers), the device records will be added to your ASM/ABM account. Once enrolled with Apple, your MDM can do the rest.

Adding an IdP solution, like Jamf Connect, **can further automate the provisioning process by augmenting cloud-based, SSO-enabled authentication**, so that devices can be shipped directly from Apple to the end user, saving considerable time and work hours. This eliminates the burden of manual configuration by IT and empowers users as they unbox their new device(s), power them on and complete the enrollment process. While users are following the streamlined user-enrollment process, secure and customized workflows execute in the background to provision their devices with the essential apps, access to services and endpoint security and configuration settings they need to be productive with minimal setup time.

Compliance reporting

For healthcare, the burden of compliance and required reporting is placed on data: health records, privacy data for patients or any information that may be used to identify a patient personally or details relating to their health history. How this data is collected, managed, shared, stored and disposed of are all subject to regulations stemming from HIPAA.

These are guidelines that health organizations are required to adhere to, however it is up to each organization to determine how they abide by these requirements as well implement and manage the necessary safeguards. Healthcare organizations need to know that PII/PHI is protected, remains protected and, in the event that it should no longer be protected, they need to take steps to respond and remediate the issue, like bring the offending app, service or device into compliance once again — and quickly!

When evaluating compliance reporting software and examining how it can **boost security while making shorter work of your compliance auditing needs**, make sure to consider:

- Logs can be collected and streamed in real-time from each endpoint to a centralized point for review by IT and security team members
- Built-in event filters examine logs to detect issues triaged by severity
- Configurable audit log verbosity levels to apply templated collection levels for a variety of device types and compliance levels
- Multiple methods to deploy and configure compliance software on endpoints to suit your organizational needs
- Customizable detection preference keys to adapt data collection to regulatory requirements
- Alignment with trusted compliance frameworks, such as NIST SP 800-53r4, NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) for managing Controlled Unclassified Information (CUI) in non-federal systems and organizations
- Integration with software solutions to centralize the collection of streaming logs (SIEM), development of policies to bring devices into compliance (MDM) and execution of remediation workflows to mitigate risks from malware and unwanted applications (endpoint protection)

“THE BEST WAY TO PREDICT THE FUTURE IS TO CREATE IT.”

– Abraham Lincoln

In this case, the future is technology advancements that permit remote access to healthcare and telehealth medicine. Although telehealth is already leveraged by healthcare providers around the globe, expanding telehealth from fully-remote consultations to hybrid models that include face-to-face visits brings with it many possibilities and its own set of security concerns.

It should come as no surprise that a device, such as a MacBook Pro or iPad, used in the field has an increased likelihood of being lost or targeted for theft and/or has a greater propensity to fall victim to data leaks by poorly developed apps or exfiltration from Man-in-the-Middle (MitM) attacks when connecting to untrusted Wi-Fi hotspots.

Malicious actors will always exist. There is no silver bullet or magic solution to stop them from attempting to exploit vulnerabilities or compromise PHI. This isn't intended to scare you, but rather to inform of a very real threat that is constantly lurking anywhere and everywhere — online, offline, at the hospital cafeteria, in patient's homes or along someone's commute. Whether healthcare providers will be subject to breaches in security is not a question of "**if**" but "**when**".

For those being attacked, this is an unknown variable. But it doesn't have to all be so dark either...

- ☑ Stay informed
- ☑ Establish ongoing training for employees on **identifying phishing attempts** and reporting security concerns
- ☑ Work with trusted partners to leverage the most **secure software solutions and services**
- ☑ Align healthcare policies with regulatory requirements and industry standard device management, security and privacy frameworks
- ☑ Consider risk assessment processes and a multi-pronged in-depth defense strategy
- ☑ Reduce attack surfaces
- ☑ Minimize risk, mitigate threats and remediate issues
- ☑ Maintain device compliance
- ☑ Safeguard users, devices and sensitive data
- ☑ Educate end users to spot the threats of today...and tomorrow.

“...TOMORROW BELONGS TO THOSE WHO PREPARE FOR IT TODAY.”

– Malcolm X

Bearing in mind the expansion of healthcare services, the known and unknown threats facing the industry, and the words of Malcom X and Abraham Lincoln — to essentially make wise decisions today that will shape and effectively create your organization’s tomorrow — presents hope and the opportunity for healthcare providers to meet today's modern security needs.

Jamf is ready to help you meet your security needs. See how with a free trial.

Request Trial

Or contact your preferred Apple reseller to try Jamf for free.