Understanding Security Frameworks

Cybersecurity plans to shore up risk and protect the enterprise from threats minimize potential attack vectors. A holistic security strategy's impact is wholly variable from organization to organization since it considers needs that are unique to each. Tying directly into needs is the role that compliance with regulatory requirements plays. This is before imagining the myriad possibilities affecting organizational security from bad actors across the modern threat landscape.

With all these variables at play, you'd think that establishing a cybersecurity plan is much harder than it seems, but it doesn't have to be.

Enter security frameworks and the benefits they provide organizations of all sizes and industries, not to mention their role in developing cohesive strategies for minimizing risk factors, maintaining compliance goals, and so much more.

Regarding the cybersecurity lifecycle, full-scale implementation and ongoing management of cybersecurity controls and solutions directly reflect the successful management of information security risks within your organization — or your failure to do so.

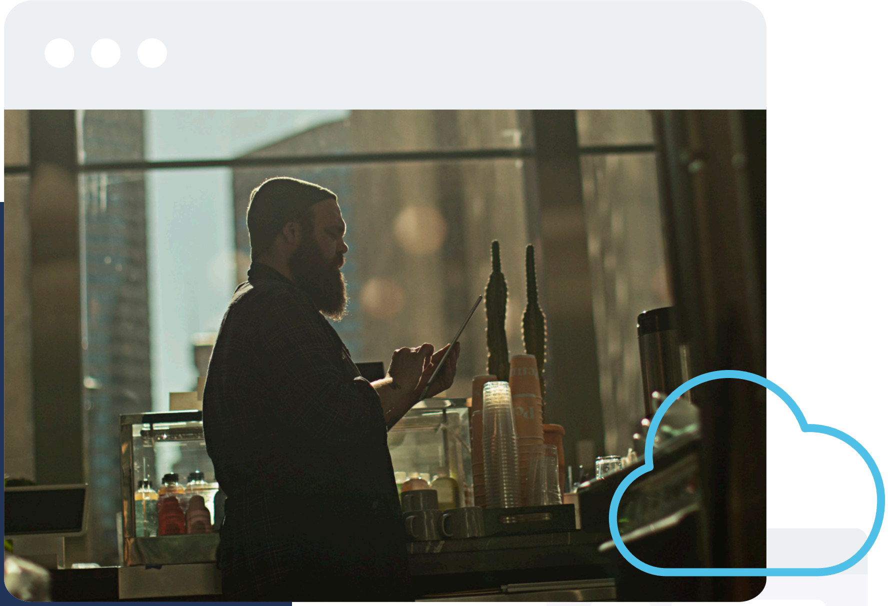
Factors that influence cybersecurity plan success are:

- The size of your organization
- Budgetary constraints
- Regulatory requirements (if applicable)
- Needs unique to the continuity of business operations
- Comprehensive and accurate risk assessments
- Knowledge base and skill set of IT and security teams

While not exhaustive, the list above highlights key takeaways crucial to any security plan's success. Even when armed with this information, organizations may find it daunting to get started, simply because there may exist **other variables that they are unaware of** or limitations to any of the factors above could result in challenges when attempting to establish the right combination of hardware, software, configurations, policies and workflows to meet your organization's unique cybersecurity needs.

Frameworks address these and many other pitfalls that may be present in information security strategies by providing a clear, concise roadmap for organizations to follow when drafting or managing their existing cybersecurity plans.

WHAT ARE FRAMEWORKS?



We used the word “roadmap” to describe the frameworks above. Another perhaps more technically accurate phrase would be “blueprint”. Much like how a contractor uses a blueprint to build a structurally sound building, IT and security teams can (and should) utilize one of the many different types of frameworks to deploy a security plan that aims to:

- Identify
- Protect
- Detect
- Respond
- Recover

The implemented frameworks should work together to mitigate cybersecurity risk through concise, organized and industry-approved best practices and methods.

TYPES OF FRAMEWORKS

There are several different frameworks. Each address and strengthen a particular component of information technology or information security. Some provide general guidance for protecting your infrastructure from current and evolving threats, and some provide information about improving processes that boost the efficiency of IT management services. In contrast, others focus exclusively on strengthening your security posture within specific security scenarios, such as regulated environments, like healthcare, finance or education sectors.

COMMON CYBERSECURITY FRAMEWORKS AND REGULATIONS

FRAMEWORKS

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1: Falling under the jurisdiction of the U.S. Department of Commerce, NIST's mission is to promote industrial competitiveness, which programs extend into various laboratories, including information technology and security. The CSF represents an ongoing collaborative effort involving industry, academia, and government to improve critical cybersecurity infrastructures whose exploitation creates financial and reputation risks.

NIST Special Publication (SP) 800-53, Rev. 5: Addresses security and privacy risks by providing a catalog of security and privacy controls for information systems and organizations from a diverse set of threats and risks, including but not limited to misconfiguration, bad actors and human error. The controls included are flexible and customizable, helping organizations mitigate risk while addressing functionality and assurance in computing systems.

ISO/IEC 27001: This standard defines requirements that Information Security Management Systems (ISMS) must meet while providing guidance for establishing, implementing, maintaining and continually improving an information security management system. It respects best practices and principles within an internationally-accepted standard that applies to companies of all sizes and industries.

MITRE ATT&CK: This is a global knowledge base of tactics used by cyber adversaries based on observations of real-world techniques. It is a foundation for developing specific threat models and methodologies across various industries, communities and endpoint security solutions.

FRAMEWORKS

American Institute of Certified Public Accounts (AICPA) System and Organization Controls (SOC): A suite of reports that span three types of reports titled: SOC 1, SOC 2 and SOC 3, and provides detailed information and assurance about the controls at a service organization relevant to security, availability and processing integrity of the systems used in the handling and processing of sensitive data while providing validated assurance of the controls by the users of those services.

Center for Internet Security (CIS): The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. Each benchmark provides secure configuration guides developed as part of a consensus-based effort of global cybersecurity experts accepted and used by governments and industries worldwide and is the foundational base in some endpoint security solutions.

macOS Security Compliance Project (mSCP): Together, the federal operational IT Security staff from NIST, National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA), and Los Alamos National Laboratory (LANL), this project is an open-source effort to provide a programmatic approach to generating security guidance, including configuration settings that deploy to attain compliance with specific regulatory goals specifically for securing and achieving compliance with Apple macOS.

REGULATIONS

Healthcare Insurance Portability and Accountability Act (HIPAA): Modernizes the flow of healthcare information and includes requirements for handling protected health information (PHI), including stipulating limitations on the disclosure of patient health data and the consequences of violating the law.

Sarbanes-Oxley Act of 2002 (SOX): This federal law enforces mandatory practices in the record-keeping and reporting of financial matters for organizations in the financial sector.

Directive on Security of Network and Information Systems (NIS): An EU mandate from the European Union Agency for Cybersecurity (ENISA) requires member states to incorporate regulations into their respective national laws to increase the level of cybersecurity protection that extends from reporting security incidents to how response teams handle them.

General Data Protection Regulation (GDPR): This privacy-focused security law was developed for Europe but impacts all organizations that handle data for EU citizen data. Compliance directives cover all aspects of user privacy, including cookie handling procedures, ePrivacy and user's "right to be forgotten," among others.

Family Educational Rights and Privacy Act (FERPA): This U.S. federal law protects student privacy and educational record data, including access to this information and the right to amend any incorrect information. For minors, this right is extended to the parent or guardian; however, when the student reaches legal age (18 in the U.S.) or attends a higher education institute, these rights transfer to them solely.

HOW TO USE FRAMEWORKS AS PART OF A COMPREHENSIVE SECURITY STRATEGY

Implementing frameworks to strengthen your security posture by addressing key factors based on best practices and sound methodologies doesn't have to be a heavy lift. It could be, but if done properly, it can be part of your security plan, integrating seamlessly with your security tooling to enforce compliance through secure processes and workflows.

There's the "old-fashioned" method of incorporating frameworks into your existing management strategy, which involves manually comparing a recent assessment of your security posture to a list of any of the frameworks listed above, for example, going down the list – point by point – to identify which configurations, settings, protocols, processes, workflows and policies do not meet compliance. And that's just the first part of the manual process. The second part involves manually correcting each out-of-scope components to bring them into compliance.

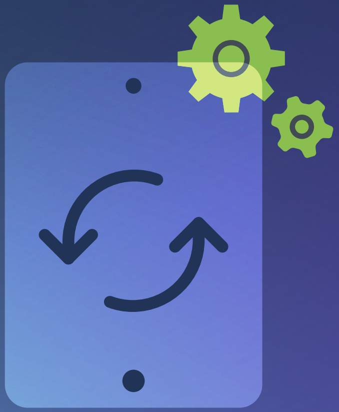
Since security is ever-changing, this isn't a "one-and-done" process either. It must be performed on a regular cadence to verify that endpoints are secured and to ensure that they remain compliant.

Challenges that significantly impact the frequency, accuracy and success of manually adapting frameworks into your cybersecurity plan are the following:

- Number and types of devices in your fleet
- Size and skill set of your IT and security teams
- Resources, like time and money, that are allotted to performing this process
- Level of support from leadership
- Competing business continuity requirements
- Impacts on user productivity, downtime and blockers
- Existing security tooling and their capabilities

With the manual process out of the way, let's shift gears to what administrators really want – an automated way of implementing frameworks into their cybersecurity plan. One that doesn't add work to already overburdened IT and security teams but instead helps:

- Shore up security concerns quickly and efficiently
- Integrate seamlessly with best-of-breed management tooling
- Add advanced workflows and policy-based management to automate mitigations
- Teams of all sizes by leveraging security tooling to perform the heavy lifting
- Free up administrative overhead, allowing the time to be better spent on other tasks
- Monitor endpoints constantly, providing real-time visibility into device health
- Cloud-based solutions allow for devices to be mitigated from anywhere, at any time
- Automate the ongoing process by dynamically adapting to changes in the security posture to enforce compliance with frameworks and evolving security needs



One way to automate the implementation of security frameworks is by using endpoint security solutions that already incorporate the frameworks your organization needs into its tooling. For example, the MITRE ATT&CK framework mentioned above can be found in certain endpoint security solutions as a foundational component. By doing so, behavioral analytics data are mapped to known threats contained within the MITRE ATT&CK database for simplified detection, and built-in mitigation workflows remediate risk as part of the ongoing monitoring process.

Another more holistic way of automating compliance through security frameworks is to leverage your Mobile Device Management (MDM) solution and the mSCP framework to generate the files necessary to achieve compliance and upload them to your MDM solution to automate and enforce compliance.

EXAMPLE

By using mSCP to build a customized baseline using the NIST SP 800-53r5 framework as the base to achieve HIPAA compliance with endpoints enrolled within your MDM, an organization can construct a baseline that meets HIPAA requirements. Their next step is to use mSCP to generate customized files:

- **Configuration profiles:** Provides configuration of managed settings customized to your organizational needs.
- **Compliance scripts:** Two scripts — one to audit managed devices for security needs and the second to perform the necessary fixes to obtain the desired level of compliance.
- **PLIST files:** These are used to check compliance standing and record audit results.
- **Spreadsheet documents:** Useful to hand to auditors and third-party investigators when determining compliance levels.
- **Report documents:** HTML- and PDF-based reports that outline each setting that is checked as part of meeting compliance, including information on what is being checked, what compliant settings should be and how to fix it.

With these files in hand, administrators can upload any custom configuration profiles (that don't already exist within the MDM) to deploy to their fleet. Uploading the compliance scripts, however, is where the proverbial magic happens. With the auditing script configured to run on your timetable, for example, once a day, the script will run on each managed daily and update the device record in the MDM with new inventory data. This will automate the critical gathering of telemetry data to know if the device meets HIPAA compliance. Next, the remediation script is uploaded and set to run as part of a policy. By doing so, administrators can limit the scope of remediation to occur automatically on only the only the out-of-compliance devices. Once the remediation script is complete, it will trigger an inventory of the device(s) to update their device records and reflect their compliant status within the MDM.

Automating compliance by integrating frameworks via your MDM solution provides the secure configuration of devices to achieve compliance goals while leveraging cloud-based management tools to enforce the security and privacy of your endpoints. Should a device fall out of scope, the automated scripts will identify which setting(s) were impacted and remediate the issue(s) — at any time, in any location and over any network connection — without IT or security teams having to handle the device physically. Integrating your MDM and endpoint security solutions via a secure API connection makes constant visibility and monitoring shareable. It supports creating advanced workflows that offer faster incident response, including Security Orchestration, Automation and Response-like (SOAR) technology, to automate the coordination of execution and remediation tasks.

WHAT SECURITY FRAMEWORKS CAN AND CANNOT DO

Frameworks are excellent for addressing a myriad of issues. We discussed what frameworks are (and are not.) Next, we take a moment to address what they can and can not do.

✓

Can

- Structure compliance requirements into organized sets of categories
- Format mitigation details with support for industry best practices and methodologies
- Act as a blueprint for organizations to follow on their compliance path
- Provide a solid foundational base for establishing a comprehensive cybersecurity program

✕

Cannot

- Protect organizations from risk or liabilities stemming from mitigated or unmitigated risk
- Be voluntary, meaning there's no mandate to implement it in whole or in part
- Explicitly prescribe solution adherence. Many compliance-based frameworks, like HIPAA, are non-prescriptive, meaning they're not explicit in their requirements of how to implement compliance best
- Provide protection themselves. They only offer guidance as to what a comprehensive security plan should look like
- Limit the length of time between updates. This could render some information outdated at best and, at worst, completely unrealistic when considering the modern threat landscape.
- Be included alongside security controls – as they are inadequate for security or compliance outside of a defense-in-depth plan
- Ensure a consistent state of compliance. No "silver bullet" solutions exist in security which also applies to frameworks. Just because your organization is compliant right now doesn't mean compliance tomorrow is guaranteed.

THE VALUE OF APPLE'S NATIVE SECURITY FRAMEWORKS

Unbeknownst to some, Apple develops its unique set of security frameworks — Apple Platform Security — supporting each operating system and working with other privacy-centric frameworks to protect the entire Apple product lineup.

They run the gamut from hardware to software, including how physical and data security is processed, handled, stored, transmitted, and accessed by users on Apple devices. And as for privacy, Apple's developed the App Tracking Transparency framework, which controls how apps collect and share data about end users to limit what is allowable while restricting what is not permissible to preserve their users' right to privacy.

Apple has been leading the charge regarding security and privacy by designing these frameworks, baking them in as part of their OS releases, and frequently updating them to stay lock-step with evolving threats that would otherwise compromise information security and user privacy.

WHERE DOES JAMF COME IN?

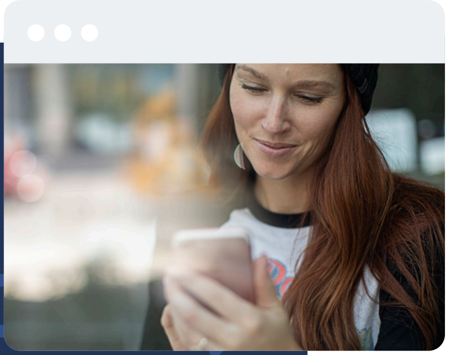
You know about Apple's commitment to security and privacy. But did you know that Jamf solutions are like an IT and Security team for your IT and security teams?

Well, we are. With our long history of supporting Apple in the enterprise, Jamf provides the solutions that help organizations succeed with Apple. Whether at work, school or play – Jamf augments the native frameworks developed by Apple by providing visibility into those frameworks, providing the answers to the questions security professionals ought to be asking about their Apple fleet:

- How are they configured?
- When are they being used?
- Why was this resource accessed?
- Who is accessing it?
- Are devices being used securely?
- What can secure them further?
- How can compliance be measured?
- What is needed to enforce compliance?

But that's not all.

JAMF HELPS YOU PUT THE THEORETICAL INTO PRACTICE



Frameworks alone don’t bolster security. Rich telemetry data can provide insight into endpoint health to determine compliance status, but that data must be actionable for risk to be mitigated and compliance to be enforced.

Our flagship MDM solution, Jamf Pro, is not just the gold standard in Apple device management because we say so – it’s because millions of managed devices globally and across all industries say so. Jamf helps organizations of all sizes to take the framework baseline and, when combined with their risk assessment data to determine data security and compliance needs, pull that into Jamf Pro to manage device configurations, minimize the attack surface through device hardening and deploy policies to aid them in not just attaining compliance, but enforcing it as well.

Through a combination of automated workflows driven by Jamf Protect — the best-of-breed endpoint security solution that’s purpose-built for Apple — IT and security teams can make short work of security and compliance needs.

Endpoint security with Jamf includes support for CIS Baselines baked right in, which means — whether your organization is just beginning to dip its toe into security and compliance waters or your team consists of veteran pros — Jamf helps organizations to secure their infrastructure quickly and from the ground up. Suppose you’re ready to take compliance and security a step further.
In that case, you can work with additional security frameworks, like MITRE ATT&CK or meet more complex compliance requirements with support for NIST and mSCP frameworks, among others.

Jamf solutions on Apple devices mean IT and security teams can focus on supporting business initiatives and providing top-tier support while ensuring that the organization’s evolving security and compliance needs are understood, addressed and remediated efficiently and effectively.

See how for yourself with a free trial or by contacting your favorite reseller.

jamf

Get Started