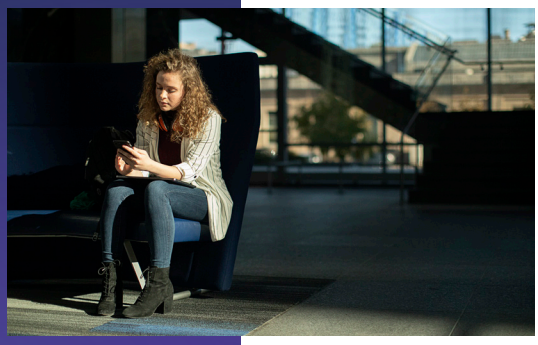
jamf

Assessing your organization's security needs



Why it's critical to your overall security posture

Understanding the unique security needs of your organization is an art form that's part theoretical part practical. Despite this duality, it has its roots firmly planted in logic by leveraging key vulnerability data gathered from risk assessments and endpoint telemetry collected through visibility and monitoring — in conjunction with knowing applicable regulatory requirements. All of these components, when combined, serve as the blueprint that drives security tooling and helps organizations achieve (and maintain) their compliance goals.

Having your finger on the pulse of your organization is paramount to its continued success. Ask any business, "How do you stay successful?" and they'll surely tell you that understanding your organization's needs and making that information actionable – by turning it into something that minimizes risks while maximizing opportunities to drive the business forward – is key. This is especially true of those that have managed to maintain operations going through economic downturns, health crises or simply kept longevity that spans decades.

In this paper, we discuss:

- What risk is and how telemetry data collected provides visibility into device health and overall security posture
- Why assessing risk must be performed at a regular cadence, iteratively as part of the security stack
- How this data aids your organization in not only determining its security needs but also how to use it to protect against current and future risks
- Why integrating risk data with endpoint security solutions helps organizations maintain a strong security posture while meeting compliance goals

This belief holds water regardless of what kind of business you run. Turn to movies and music, for example. Entertainment has existed throughout the centuries. And to varying degrees, it's stood the test of time by being able to assess what its target audience wants while transforming its offering to meet the demand.

It's an ongoing and evolutionary process.

And along similar lines, cybersecurity operates on much the same frequency. Instead of assessing the demands of your customers, however, organizations must look inward to determine what's required to continue safe, secure business operations. Risk assessment includes everything from devices to software and your organization's infrastructure, data, processes and policies. These pieces come together to complete the picture of an organization's security posture.

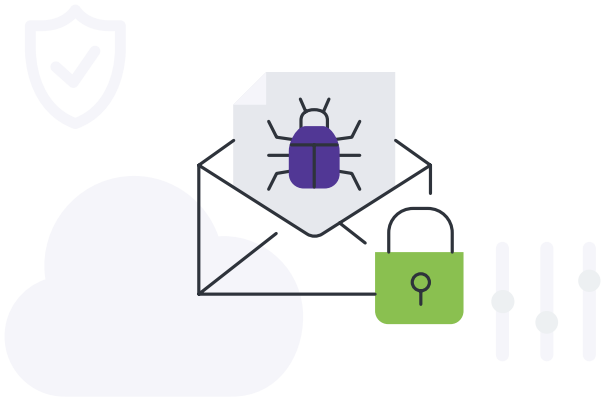
Armed with this information, organizations can assess the risks and liabilities of their current cybersecurity strategy and take the necessary steps to correct them, minimizing risk and mitigating threats.

Risk assessment is not is a "one-and-done" process. In accordance with best practices, risk assessments should be done on a regular cadence. Because of the dynamic nature of technology, everything's always in a transient state. This is even more important for security because bugs are a naturally recurring issue that lead to vulnerabilities that lower the security posture and ultimately place devices, users and data at risk of compromise.

This is not taking into consideration threat actors that actively probe and test your network's defenses for signs of weakness and attack vectors to exploit.

Simply put: risk assessment should be performed regularly as part of a comprehensive cybersecurity strategy where the assessment data gained is not only used to inform the current state of security but also to iteratively inform the organization's holistic defense-in-depth security plan, such as:

- Stages in the device and application lifecycles
- Procuring, configuring and deploying security controls
- Meeting regulatory goals and enforcing compliance
- Identifying existing and new threats, and assigning criticality and severity levels
- Maintaining alignment between risk appetite and mitigation strategies
- Revising and implementing incident response procedures
- Updating and instituting threat prevention strategies, like end-user training



Risk assessment

We've discussed why risk assessments are important, but what does one look like? And what's actually at risk? While the exact details can vary from industry to industry or company to company, it boils down to understanding:

- The threat landscape
- Your organization's vulnerabilities
- The likelihood of an attack
- The impact an attack will have on your organization
- How quickly your organization can recover from a serious attack

> *"To know your enemy, you must become your enemy."* **— Sun Tzu**

Let's look at some questions that a risk assessment has to answer.

Where is my organization vulnerable?

An attacker can use many points of entry to exploit your system, such as hardware, software, interfaces and vendor interactions with your network infrastructure, as well as any user who has access to these components. Vulnerabilities can also crop up in your business processes and policies.

Classifying and inventorying these components is necessary to have a solid understanding of your infrastructure. You should know:

- What devices are accessing your network
- Who has access to your data
- If you're following security best practices (e.g., least privilege access, strong password policies, etc.)
- If your vendors introduce vulnerabilities to your systems
- If users are trained on recognizing potential threats and practicing good security hygiene

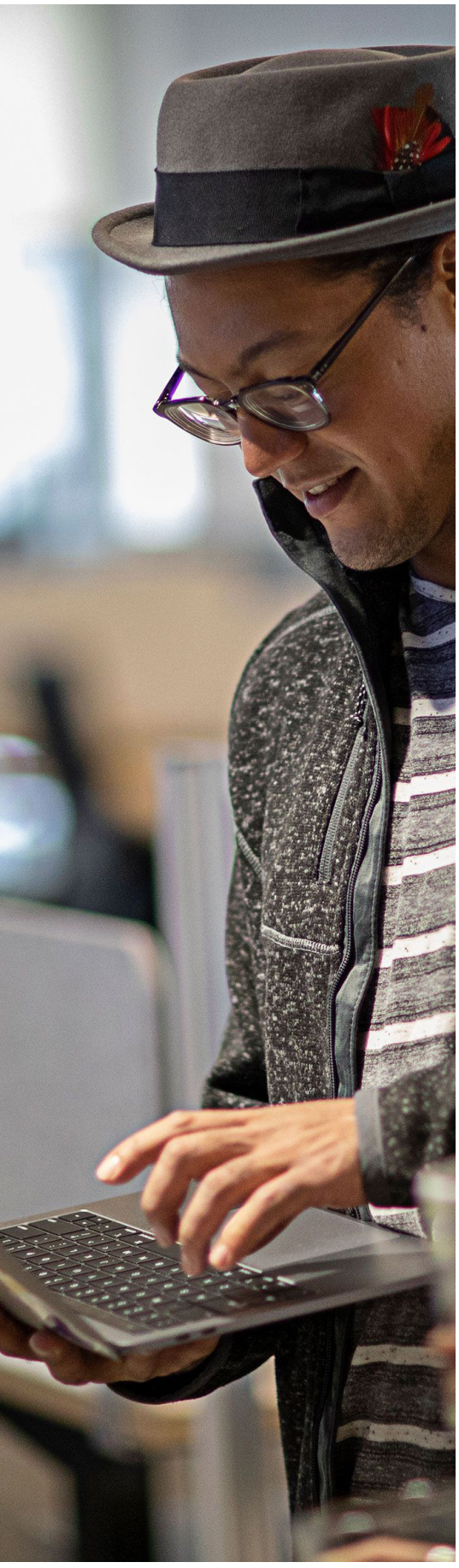
What threats are out there?

Assessing risk also means knowing what threats are out there and how they can affect your system. This helps your IT and security teams evaluate the most vulnerable part of your organization, how likely an attack is and what impact it could have on your business.

EXAMPLE

Referencing the MITRE ATT&CK framework gives Security teams the information they need to understand how bad actors could attack your system. And for unknown threats, teams can consider threat hunting and the use of AI and machine learning (ML) software to identify suspicious or malicious behavior. AI and ML work tirelessly behind the scenes to identify anomalies outside your network's baseline behavior. Their ability to process enormous datasets of threat intelligence and pattern-matching data makes these critical tools in your cybersecurity arsenal. Additionally, the data gleaned from this software can be shared with the larger security community, further enhancing cybersecurity professionals' threat knowledge base everywhere.

Knowing common threat vectors can help you prioritize what parts of your organization need defense most. Threats come in many forms — according to **Verizon's 2023 Data Breach Investigation Report**, attackers infiltrated organizations with stolen credentials, phishing and exploiting vulnerabilities. Generally, the source of data breaches comes from totally external sources, but a non-trivial amount (as much as 40%) comes from the exploitation of partner software. Defending against these threats requires thoughtful analysis of your current setups and policies — more on defending against these later.



What impact would a cyber attack have on my organization?

Understanding the likelihood of a threat helps with prioritization in your defense strategy. But another part of this is understanding the impact a threat has on your organization's mission, which can be financial, with the average total cost of a data breach at 4.35 million USD in 2022, according to **IBM's Cost of a Data Breach Report**. It can be time lost, with an average of 277 days to identify and contain a breach. Or it can hurt your relationship with customers, whether via reputation or by increasing customer prices due to data breaches as 60% of affected organizations did in 2022. Not to mention any fines from governing organizations if your company is not compliant with applicable standards.

What's next?

Naturally, the larger the impact of an attack, the higher the priority to defend relevant systems. This is also true for attacks with higher likelihood. The combination of these two metrics — impact and likelihood — helps quantify how risky certain threats are to your organization. A solid understanding of the risk gives you the knowledge needed to prioritize and determine the following:

- What critical systems need the most protection (i.e., will cause the greatest loss toward mission-critical functions)
- What controls to implement for the best defense strategy
- What software tools can enhance your security posture
- How much risk you can tolerate (i.e., your risk appetite)

Once you have the information from your risk assessment, it's time to implement what you've learned. In the next sections, we'll address evaluating your network and device telemetry and what guidelines you can use when developing or revising your security policies.

Visibility and monitoring

So, you've assessed risks, identified them and adjusted your risk appetite to align with your tolerance level. Additionally, you've made the necessary changes to procure and configure security controls to mitigate risk. Your security posture is strong and stakeholders have received the requisite training to identify current threats while understanding that they need to be reported and acted upon. Endpoints are secured from threats and compliance goals have been achieved, with all devices falling within scope. Now what?

Are IT and security teams simply done with their work and can take an early (and likely much-needed) holiday? Sadly, no.

Once again, the dynamic nature of technology is ever present, and in this case, it means that just because something is secured right now, today, doesn't mean it will forever remain secure. The key to keeping your devices, infrastructure and your organization safe from pervasive security threats lies in the understanding endpoint health statuses at any given time.

> *"We are not fit to lead an army on the march unless we are familiar with the face of the country..."*
> **– Sun Tzu, The Art of War**

The telemetry data recorded from actively monitoring device health status contains a wealth of information for maintaining device and organizational security postures. Not just that, but when speaking of compliance, telemetry data is the key ingredient to ensuring that endpoints are configured properly to meet regulatory requirements and providing the metrics by which organizations can prove that endpoints were compliant at any given time — a critical requirement is showing proof of compliance when seeking regulatory certification, like **PCI-DSS** for organizations to be able to accept and process card payments securely.

Of additional importance, visibility gleaned through monitoring informs decision-making at all device levels and application lifecycles. The nature of the monitoring process serves to provide IT or Security teams with up-to-date information regarding the health of their devices, the software running on them, and the actions taken by end users. But it also provides administrators and management with rich telemetry data to iteratively make informed determinations relating to any adjustments needed to ensure devices remain compliant and that users and data stay secure.

What kind of data does monitoring collect?

Before diving into the types of telemetry data gathered through monitoring, let's first discuss the two types of monitoring:

- **Passive:** Health data is gathered slowly, usually over a period of time to minimize any impact on the end user or the performance levels of the monitored device. The infrequent nature of the data capture means it can take more time to collect telemetry data and, therefore, delay the creation of a fully-formed device baseline. Also, any delays in data gathering could directly impact the accuracy or timeliness of the data, especially if days or months pass between data captures.

- **Active:** Health data is communicated from endpoints frequently. Endpoint polling occurs regularly and is transmitted to a centralized repository, often in real time.

Though nearly identical in terms of what data is captured, the major differences between both are:

- **How** telemetry data is captured
- The **length of time** in which it takes to build a baseline profile
- The **accuracy** of the information
- And the **frequency of updates** to the telemetry data

While both types of monitoring provide their pros and cons, the fact remains that the modern threat landscape is both too vast and changing too rapidly for anything other than active monitoring to be an effective means of gathering the most up-to-date device health data and converting that into actionable data to fill the gaps in your security plan, as summed up by the security axiom, "You can't protect what you can't see," in SecurityWeek's writeup on **Active vs. Passive Monitoring: No longer an either-or proposition.**

Types of telemetry data collected and what it means for your security posture:

- **OS updates:** Determine operating system (OS) update levels to know devices support the newest features and if devices have the latest protection against known threats for minimizing vulnerabilities.
- **App patch levels:** Like the OS, apps require patches to protect data during processing while fixing bugs and mitigating vulnerabilities that could otherwise introduce risk.
- **Configuration settings:** Hardening devices is critical to the security posture. Not just because you want to configure them for maximum security correctly but also to minimize the possibility of misconfigurations, which **contribute to 21% of error-related data breaches (Verizon Data Breach Investigation Report 2023).**
- **Network activity:** With what web-based content are devices communicating? Are untrusted connections being secured? Which ports are transferring data? Answers to these and other important questions surrounding network utilization are critical to determining the security posture of your devices.
- **Behavioral analysis:** Users are considered the weakest link in the security chain for good reason. Varying levels of understanding contribute to the continued success of social engineering attacks. By understanding how users perform on their devices, administrators get a clearer picture of how user-introduced risks occur and, therefore, how to better protect against them.
- **Authentication auditing:** Authentication protocols and password management are keys that unlock a device and its sensitive data. A bigger, stronger lock or complex password scheme doesn't reveal if users are sharing credentials or have had their accounts compromised – this goes double for remote and hybrid work environments where a distributed workforce relies on policy-based management to enforce security on remote endpoints.
- **Malicious code:** The presence of malicious code can occur in various forms. From downloading a trojan disguised as a legitimate app or sideloaded apps, to unknowingly visiting a compromised website to seemingly dormant threats running in the background – any of these can potentially compromise compliance, especially considering growing adoption and attack trends related to mobile devices.
- **Error logging:** Devices log everything, and the more devices administrators are responsible for, the harder it is to address every issue logged. This is great for threat actors and bad for admins. Still, it doesn't have to be. When managed properly and leveraging Security Information and Event Management (SIEM) solutions to sort and make sense of the potentially overwhelming telemetry stream, error logging and threat detection is not only effective but also efficient.
- **System processes:** Endpoint security administrators must know what apps run on their devices. This speaks to the average baseline of the device itself and alerts admins to the usage of unsanctioned (Shadow IT) or disallowed (Restricted) tools that may otherwise lower security by allowing for data leaks to occur or **increase risks to user privacy.**
- **Audit compliance:** Endpoint health visibility is as much about what is known as it is about what is not. With regulated industries, an organization's ability to know where they stand on their compliance path means understanding what's necessary to achieve compliance goals while collecting evidence of this achievement.

But can telemetry data be used to mitigate risk automatically?

Why yes, yes, it can. As a matter of fact, in light of several factors that make managing risk significantly more difficult, like:

- Ordering large quantities of devices, different device types
- Maintaining security across a fleet of personally and company-owned devices
- Supporting distributed workforces in remote and hybrid environments
- Convergence of two or more threat types to execute complex, multi-pronged attacks against targets
- Enforcing security settings to maintain endpoint compliance

Automating the collection, analysis and sorting of telemetry data is preferred to going through each stage manually. Given the sheer volume of data to comb through, the quantity of time in completing each as quickly as possible and, of course, the limitations that humans can only do so much before requiring breaks for food and rest.

None of these significant limitations apply to computers.

Leveraging systems to perform the “heavy lifting” through automation saves organizations precious time and money — resources better served to prevent attacks from occurring successfully than scrambling to clean up in the aftermath.

Active monitoring is the second layer (after risk assessment) in your security plan to understand your organization’s security needs. Telemetry data is gathered and delivered in real time by continuously monitoring your fleet, which provides up-to-date endpoint health data that is analyzed and processed by your endpoint security solution to determine how each device stacks up. Any deficiencies that are detected or anomalous behaviors that are flagged can be automated to send alerts to IT or security teams (at the very least) to determine next steps. The detections can also be used to initiate automated workflows for handling incident response, like automatically removing known suspicious software from devices or quarantining endpoints infected with ransomware, for example.

Other, more advanced workflows are possible by further integrating endpoint security solutions with other tooling, such as identity and mobile device management (MDM), to create robust workflows that offer greater automation capabilities.

Compliance

Various quotes from Sun Tzu's, The Art of War, are scattered throughout this paper to help tie together a few central themes that IT and security professionals may find useful as they perform due diligence to assess risk and prepare to understand their organization's security needs better. The intention is to bridge any gaps while establishing the understanding that each stage is critical in its own right. Furthermore, each leads directly to the next phase by taking the information present and using it to inform the next steps.

Understanding your security needs doesn't just mean knowing what security issues are present at a given time. It means identifying what is needed to resolve issues and which strategies to choose to ensure that your endpoints remain in scope with your compliance needs – regardless of whether your organization is part of a regulated industry or not. The goal is to remain compliant with your regulatory requirements, or for non-regulated businesses, to maintain alignment with organizational policies — both serve to uphold security and user privacy by mitigating risk using a structured framework that keeps your device and organizational security postures strong.

> *"The supreme art of war is to subdue the enemy without fighting."* **– Sun Tzu**

The "enemies" in this case are threat actors and anything or anyone that can introduce risk into your organization. After all, risk equals a liability that could otherwise lead to exploiting a vulnerability or far worse consequences. When it comes to understanding your security needs, however, it is futile to worry about the multitude of potential "enemies" above your network's immediate, more concrete state. Your attention is better served on the variety of risks themselves and not from where they orginate. Doing so, in turn, helps administrators maintain the focus on how best to move forward to maintain compliance by keeping devices, users and data protected against both current and growing and evolving threats.

Which industry guidance help to identify and minimize different types of risks?

It's important to distinguish between guidelines, frameworks and baselines before proceeding. Guidelines share an affinity with best practices. There are not always hard rules to follow, but rather a grouping of industry practices to help organizations manage various forms of risk at a general capacity.

On the other hand, frameworks sharing a similar DNA as best practices aim to concatenate all of the information, practices, settings, controls and workflows necessary to meet or exceed a specific organizational or compliance goal.

Baselines share similarities with the two former guidance types for their role in achieving and maintaining compliance but from a different angle. Guidelines provide ideas for best practices and frameworks organize them in a structured way, formatting them to achieve a particular endgame, but baselines aren't implemented in the same way. They act as barometers that organizations can use to measure their level of success in achieving their compliance or organizational goal.

In lay terms, guidelines are like ingredients. Frameworks result from combining elements to create a certain type of dish. Lastly, baselines act as judges to determine if the dish was prepared properly, according to the ingredients used and recipe followed. And voilà, bon appétit.

Now that we understand the differences, we move forward with frameworks and baselines since we aim to understand our security needs and address them as accurately as possible.

Frameworks commonly used in security planning

National Institute for Standards and Technology (NIST) SP 800-53, Rev. 5: Security and Privacy Controls for Information Systems and Organizations, provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets...from a diverse set of threats and risks.

NISTIR 8011, Vol. 4: Automation Support for Security Control Assessments, focuses on the automation of security control assessment within each individual information security capability while it simultaneously addresses the management of risk created by defects present in software on the network.

ISO/IEC 27001: Information Security Management Systems (ISMS), is among the best-known standards for defining requirements that must be met by an ISMS. The framework provides holistic guidance for establishing, implementing, maintaining and continually improving an information security management system.

Cyber Essentials: A U.K.-based initiative that guides how to protect your organization, whatever its size, against a whole range of the most common cyber attacks. It offers multiple tiers, including hands-on technical verification to ascertain compliance.

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

Control Objectives for Information and related Technology (COBIT) 2019: A framework created by ISACA that focuses on and defines generic processes for IT management and links them to business and IT-related goals. This includes a measurement component to ensure team accountability while flexibly allowing tie-ins with other frameworks, like ISO 27001, ITIL and popular project management frameworks.

Payment Card Industry Data Security Standard (PCI-DSS): The de facto information security standard organizations use that govern the technical and operational requirements of handling credit card payment data and is enforced by major card issuers globally.

Cybersecurity Maturity Model Certification (CMMC) 2.0: Based on the security requirements from several NIST special publications, the multi-level model provides certification levels for organizations that cumulatively meet CMMC levels and associated sets of practices across domains.

OWASP Risk Assessment: Consisting of security testing, risk assessment and scanning tools, this framework by OWASP seeks to eliminate the uncertainty stemming from compatibility and complexity related to environmental setup processes to allow a simple way to analyze and review their code quality and vulnerabilities without any additional setup" as well as "help developers to write and produce secure code.

macOS Security Compliance Project: The joint project of federal operational IT Security staff from NIST, National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA), and Los Alamos National Laboratory (LANL) is an open-source effort to provide a programmatic approach to generating security guidance, including configuration settings that may be deployed to attain compliance with specific regulatory goals.

The role of baselines in cybersecurity

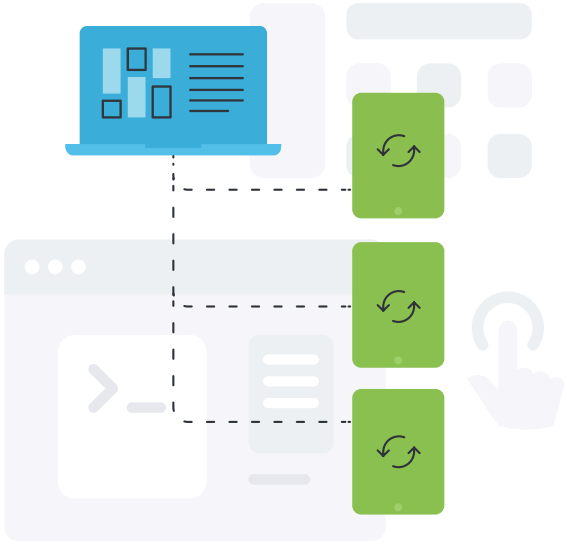
Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs): A configuration standard managed by the U.S. Department of Defense (DoD), STIGs contain specific requirements for securing computing systems -- from logical designs to protocols that run on hardware appliances to the software that runs on them, these guides aim to "enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities."

Federal Information Processing Standards (FIPS) 200: Also developed by NIST for the U.S., these standards are for in non-military computing devices and systems used by the American government and contractors. While the FIPS standards cover a range of security baselines, FIPS 200 provides standards to ensure that data used by or on behalf of federal agencies meet the minimum information security requirements for each category in the objectives, ensuring the appropriate levels of information security according to a range of risk levels while classifying the impact levels for **security objectives based on the CIA triad.**

NIST SP 800-39: Broad-based guidance useful when integrating with a comprehensive Enterprise Risk Management (ERM) solution. The document provides specific details of assessing, responding to and monitoring risk on an ongoing basis in conjunction with other standards, guidelines and frameworks.

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

Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs): Developed in coordination with CISA, NIST and the interagency community, these CPGs act as broad baseline cybersecurity performance goals that are consistent across all critical infrastructure sectors... especially help small- and medium-sized organizations kickstart their cybersecurity efforts while serving as a benchmark for the measurement and improvement of cybersecurity maturity.



Risk assessment + continuous monitoring + security guidance = compliance managed.

> *"Know yourself and you will win all battles"* **– Sun Tzu**

Each of these components on their own can only serve organizations to an extent, but join them together, and not only will you be able to:

- Determine your liabilities
- Know endpoint health-status levels
- Minimize the attack surface by hardening settings
- Achieve your compliance goals

But you will also be able to maintain compliance by establishing baselines and then measuring against them by with proactive monitoring and reassessing rich telemetry data, completing the loop to improve the security posture of your devices continuously – and that of your infrastructure overall.

As mentioned, it's an iterative process – not a static one. The loop mentioned above does not close once it is achieved. Still, it continues to cycle, touching upon and informing each phase, security control, processes, workflow, requirement, policy and setting configured for each device, end user and sensitive piece of data in your organization.

Whether your organization is in a regulated industry or you're a business of any size that is not regulated but still wishes to align its cybersecurity strategy to organizational policies and administrative controls — like Acceptable Use Policies (AUPs) — think of each of the core components as cogs in the wheel that form together to provide a greater understanding of your security needs and the information necessary to fill the gaps.

You may be thinking, "I'm a MacAdmin. I know what risks exist within my organization and I'm drowning in device health data. Furthermore, this guidance highlights the discrepancies between where we currently are and where we need to be to obtain compliance. What now?! How do we go from here to there?"

Enter Jamf

Helping organizations to succeed with Apple.

More than just a catchy phrase, those words represent Jamf's mission statement. And more to the point – it's just what we do. Jamf isn't the gold standard for Apple at work simply because we say so. What gives Jamf this reputation is the best-of-breed solutions we develop that help countless organizations successfully manage and secure millions of devices across all industries worldwide.

It's the support we provide to ensure that you're maximizing your potential with Apple products at work. How do we provide you with the tools to comprehensively and holistically manage your Apple fleet while identifying, understanding and meeting your unique organizational needs and compliance goals, you ask?

Take the guesswork out of endpoint validation.

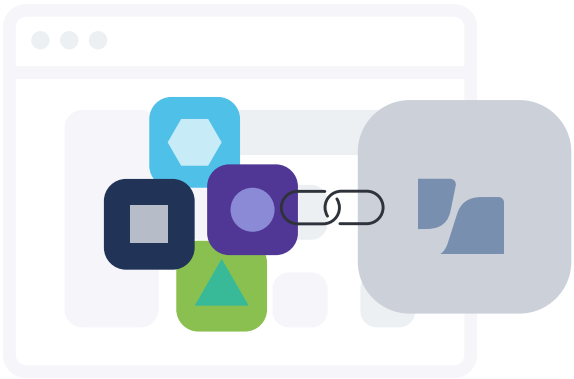
A considerable part of understanding your security needs involves knowing the status of the endpoints in use within your organization. Without rich telemetry data to verify each device's health status, administrators have little more than conjecture to work with— and a guess at best or an ill-judged miscalculation at worst — have the potential to spell disastrous consequences.

As administrators, **you don't just want to know but rather, you need to know.** And when it comes to compliance, whether enforcing regulations or alignment with organizational policies, you also need to verify endpoint health status at any given time to ensure the needs of the organization are being met every step of the way.

Social engineering is a key attack vector targeted by threat actors that exploits your risk. More specifically, social engineering exploits an organization's current risk and introduces greater risk through compromising credentials or passing on malicious code when infected devices connect to business resources.

Technologies like **Zero Trust Network Access** (ZTNA) keep your devices protected by checking endpoint health against a series of requirements to ensure devices meet a minimum level of security before access to requested resources is granted. Adhering to the "never trust, always verify" creed, a ZTNA solution, like **Jamf Connect**, verifies that access is originating from an enrolled and trusted device, making identity and access management a corner stone of your security strategy.

Endpoint security solutions, like **Jamf Protect**, add a safety net to your macOS, iOS, iPadOS, Android and Windows devices to ensure that they (and the users relying on them to stay productive) are safeguarded against suspected threats, like preventing malware and more, through analysis of on-device and in-network threats for faster detection, quicker incident response and effective, automated threat mitigation and remediation **workflows that don't compromise security, privacy or performance.**



Spread love and trust across your infrastructure.

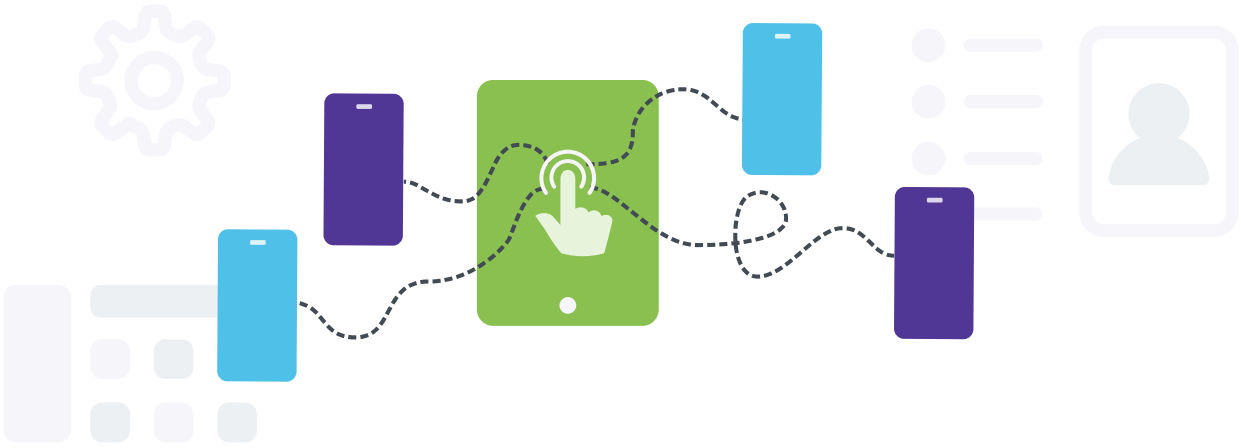
Your needs don't begin when a device connects to business resources for the first time – it starts before the device is even unwrapped. Let us explain.

Zero-touch deployment refers to a process by which **devices are ready to use the moment the end user powers on their device** for the first time. This deployment workflow automatically and securely integrates Apple Business Manager or Apple School Manager with Jamf.

Whether it's company-owned devices or personal devices belonging to end users, **Jamf Pro** supports multiple ownership models, like bring your own device (BYOD) to user enrolled devices, ensuring security while upholding user privacy. And speaking of security, our MDM solution offers administrators **same-day support for all Apple features, including security and privacy enhancements**, so you can support and manage the functionality that helps users work smarter, not harder, without making compromises or exceptions to endpoint security.

Application management is a critical part of your security needs. Deploying updates to operating systems (OSs) and applications is table stakes to the success of any security plan. After all, what good is understanding your security needs if you can't do anything to remediate issues when they arise? Once again, Jamf Pro shines by **helping MacAdmins to make short work of the app lifecycle management** with bulk management commands to keep devices up to date with OS updates. And don't forget the apps! Jamf's **Self Service** app catalog, along with the power of App Installers, ensures the apps your end users need are easily accessible, always managed, automatically updated to the latest versions and in their most secured state.

Streamlining identity and access provisioning is a tentpole to a comprehensive, defense-in-depth security strategy. Enforcing trusted access by ensuring that only trusted users can access devices and resources from anywhere at any time makes all the difference when managing devices, especially in distributed workforces. This sets up users for success by offering them an easy way to authenticate to their devices — from a seamless onboarding experience from zero-touch deployment to day-to-day work work and accessing business resources. ZTNA and conditional access with **Jamf Connect** further enforces the paradigm that **effective, adaptive and flexible security isn't optional.**



Three essential security elements – one trusted platform

> *"Opportunities multiply as they are seized."* **— Sun Tzu**

Trusted Access is a holistic approach to security that delivers a comprehensive solution that supports the management and security needs of every organization across all industries.

Each element of Trusted Access — **device management**, **endpoint protection** and **visibility and compliance** — are crucial for an effective, defense-in-depth security strategy. One that layers advanced access controls and secure configurations for devices, users and data while leveraging telemetry data to adapt to any changes in the security posture or your devices or organization to maintain security, preserve privacy and remain compliant.

Flexibility plus security for your entire Apple fleet anytime, anywhere minus the complexity.

Contact us to learn how Jamf help you assess your security needs with our best-in-class solutions.

Get Started

Or contact your preferred reseller to take Jamf for a free test drive.

jamf

www.jamf.com