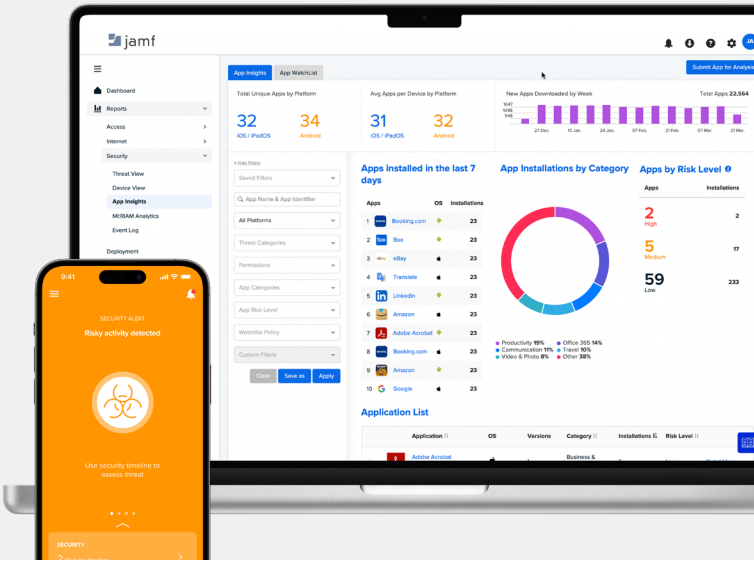
jamf

Best Practices:

Enterprise Threat Defense



Security means many things to different companies. Risks classified as critical in one organization may hold lower significance in another organization or industry – not because the former takes security more seriously than the latter – but simply because of the compliance needs that may be unique to each organization and their respective industries.

Beyond the differences in classifying and prioritizing risk factors between organizations, there is common ground shared by all enterprises about their cybersecurity plans: the aim is to strengthen your security posture.

A key to achieving this within your enterprise is augmenting your cybersecurity plan with proven threat-defense strategies. Each of the strategies we dive into in this technical paper are not just industry-recognized best practices when used independently to provide crucial confidentiality, integrity and availability of endpoints and sensitive data, but when combined, helping organizations to reap the following benefits by implementing the solutions we talk about in this guide:

- Develop a defense-in-depth strategy
- Extend layered protections across your infrastructure
- Streamline Mac and mobile endpoint management & security
- Maintain compliance with data security and user privacy
- Minimize complexity, by consolidating IT and Security workflows
- Speed-up incident response while increasing user productivity and ROI

1. Data encryption

We begin our roundup with encryption. While it's often referred to as the last line of defense, enabling volume encryption on all device types provides a layer of protection against unauthorized access by threat actors should other lines of defense fail to prevent attacks. The algorithms that makeup encryption may be complex, but luckily for administrators, deploying the security feature is simple and easy to manage when configuring it from your mobile device management (MDM) solution.

Administrative workflows include checklists of best practices. Setting up an admin account and password across all IT-managed devices, managing user permissions to unlock encrypted volumes and maintaining accurate records of each device's unique recovery key represent tasks that provide significant protection against unauthorized data access but, given their complexity, added administrative overhead and introduced errors into the process because of its manual nature. The variety of operating systems (OS) supported multiplied by the number of devices equals the greater the challenge of keeping this crucial information accurate.

Enabling volume encryption from your MDM solution simplifies the deployment of data encryption workflows on devices by:

- Ensuring consistent enforcement across Apple device fleets running macOS, iOS, iPadOS, watchOS, tvOS and visionOS.
- Achieving security parity between company-owned and BYO devices while upholding user privacy.
- Automating encryption workflows and enforcing seamless protection from the moment devices complete the setup process during onboarding.
- Creating admin-level accounts upon successful enrollment and using Local Administrator Password Solution (LAPS) for Jamf Pro to store, rotate and view randomized passwords for managed, local admin accounts.
- Centrally managing recovery keys within a device's unique record for secure storage and easy access if needed.

2. Regular patching and updates

One of the most effective ways for organizations to protect their devices, users and data is to keep their devices current with security updates and system and application patches. While zero-day threats have grown in both frequency and impact levels, our focus in this section is on known vulnerabilities and bugs found in code that have existing patches/updates available from the developer to fix the issue and the criticality that a regular update cadence plays in keeping your device and organizational security posture strong.

The important thing to keep in mind about known vulnerabilities is the term “known”, as in, there’s an update available to mitigate the risk the vulnerability poses to organizational data and compliance requirements. Bearing this in mind, there are a number of methods built-in to MDM to help not only keep devices secured against known threats but further bolster native OS security protections by unlocking new features and functionality that often are included with the latest updates, benefiting organizations by both maintaining data security while keeping end users productive.

Some of the flexible ways that MDM solutions ensure devices remain up to date are:

- Support for same-day OS updates and upgrade workflows means organizations can patch devices on their timetable – not ours.
- Managed apps are always kept current when deployed from the Apple App Store, for third-party apps that aren’t, Jamf App Installers automates the update process for 700+ applications in the Jamf App Catalog.
- Maintain regulatory compliance by enforcing OS requirements through policy-based management.
- Integrate with Jamf Connect, enabling Zero Trust Network Access (ZTNA) that keeps protected resources secure from compromised devices, triggering automated remediation workflows.
- Manage and secure endpoints from a centralized, holistic solution that provides converged teams the visibility they need into device health with the tools necessary to make updates actionable based on real-time telemetry data.

3. Multi-Factor Authentication (MFA)

When discussing identity and access management (IAM) and defense-in-depth strategies, MFA is the logical progression when implementing security controls to verify that users are who they claim to be during authentication. Verifying credentials is one-half of the zero-trust model. The established method of relying solely on user credentials to limit access to sensitive resources has been proven ineffective against passwords that are easily guessed or the minimal protection provided bypassed entirely by threat actors that mine credentials effortlessly from highly successful attacks, like phishing campaigns.

According to the Cybersecurity and Infrastructure Agency (CISA), "The use of MFA on your accounts makes you 99% less likely to be hacked." This statistic is echoed by organizations such as Microsoft and Google to prevent 99.9% of attacks on your accounts and block around 99.9% of automated bot attacks, respectively. This underscores how critical MFA is to your security stack but also how crucial it is to:

- Extend the same level of security to all endpoints regardless of their ownership model or whether users work as part of a distributed workforce or from the office.
- Minimize credential-based threats, including preventing unauthorized access to protected resources – even in the event of compromised passwords.
- Integrate alongside other controls, functions and services as an additional layer of defense against the modern threat landscape.
- Reduce authentication risks by implementing passwordless workflows, replacing easily guessed passwords, with two or more verification factors that are difficult to bypass.
- Simplify the user's experience during device provisioning or accessing enterprise resources by automating the authentication experience through Single Sign-On (SSO) and passwordless security with just their mobile device.

4. Zero-trust architecture

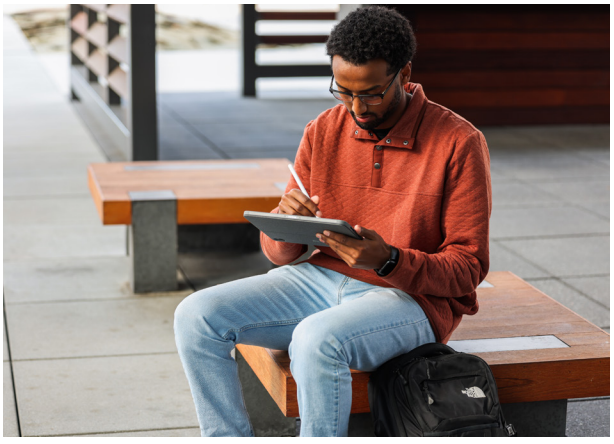
Regarding the critical role integrating identity plays within your security stack, no discussion is complete without Zero Trust Network Access and how the model, based on zero trust, applies the next generation of IAM to restrict access to verified users and compliant devices only – all others are denied, by default.

The modern threat landscape mirrors the current computing landscape in that the latter has changed how work is performed in the enterprise. Whether working at the office or as part of a distributed workforce, on a Mac computer or mobile device that could be personally or corporate-owned – productivity needs to occur from any device, at any time, from anywhere and over any network connection securely.

Just as organizations need to adapt to hybrid work environments, so too must security evolve so that devices, users, data and the network connections they communicate over remain secure despite the many challenges and threats, like the **147%** uptick in global cyberattacks targeting mobile devices from December 2022 to 2023.

Some of the ways ZTNA helps prevent Mac and mobile OS threats in the enterprise are:

- Devices, data and resources are protected yet separate. This means every resource request remains denied by default until device health is verified, keeping data secure by ensuring that credentials are free from compromise and devices are compliant before access is granted.
- Cloud-based infrastructure easily integrates and extends consistent threat defense across desktop and mobile fleets alike without complex equipment or configurations to manage, streamlining security regardless of the OS, device type or ownership model of devices used for work.
- Secure all network connections using micro-tunneling that isolates each request to prevent network-based threats, like Man-in-the-Middle attacks while adhering to the principle of least privilege, granting encrypted access to just the resources users have permission to access (unlike legacy VPN solutions that provide implicit access to your entire network).
- Leverage context-aware access policies to enforce compliance with company and/or regulatory requirements or allow/deny access based on requirement attestation, such as OS/app patch levels.
- Always-on protection ensures that business data remains safe while split-tunneling intelligently routes personal data directly to the internet. Uphold user privacy without compromising security, or vice-versa.



5. Vulnerability assessments

At the risk of sounding like we're inflating importance, risk assessments are about as critical as they come in the IT and Information Security space. Beginning with the fact that how can you possibly expect to keep something safe when you haven't discovered what that "something" is? As part of a vulnerability management program, the process of assessing what risks and vulnerabilities impact your organization is a crucial first step that informs each subsequent part of the process. Ultimately, it informs and is iteratively informed by each control, process and workflow at each layer of s comprehensive, defense-in-depth cybersecurity plan.

The vulnerability management process occurs over five stages, but in this section, we focus on the first two:

1. Identification
2. Assessment
3. Prioritization
4. Resolution
5. Reporting

We touched upon why identification is critical – you can't protect what you don't know. With an MDM solution, this process kicks off with your inventory to discover the devices and any relevant variables that could impact your security posture. Some examples are:

- Device type
- OS version
- Apps installed
- Hardening configurations
- Endpoint security software installed
- Ownership model
- Assigned users

The next stage, assessment, relies on your endpoint security solution's ability to determine the health status of each device that touches your infrastructure. Combining device scans, logging data and the inventory shared by your MDM, admins armed with this telemetry data compare current endpoint health in real time to baselines to determine if any security gaps exist, for example:

- Operating systems are not updated to the latest version
- Installed apps are affected by known vulnerabilities
- Devices are missing security configurations or misconfigured
- Network connections on remote user devices are insecure

6. Endpoint Detection and Response (EDR)

When risk is identified and assessed, what follows next are the final three stages of vulnerability management, which pivot from gathering and analyzing data into actionable tasks that mitigate threats before they spread further.

Continued from above, stage three is prioritization. Here, admins and/or endpoint security software augmented with artificial intelligence (AI) sort findings into classifications for vulnerabilities and risk factors identified to determine the impact on the enterprise.

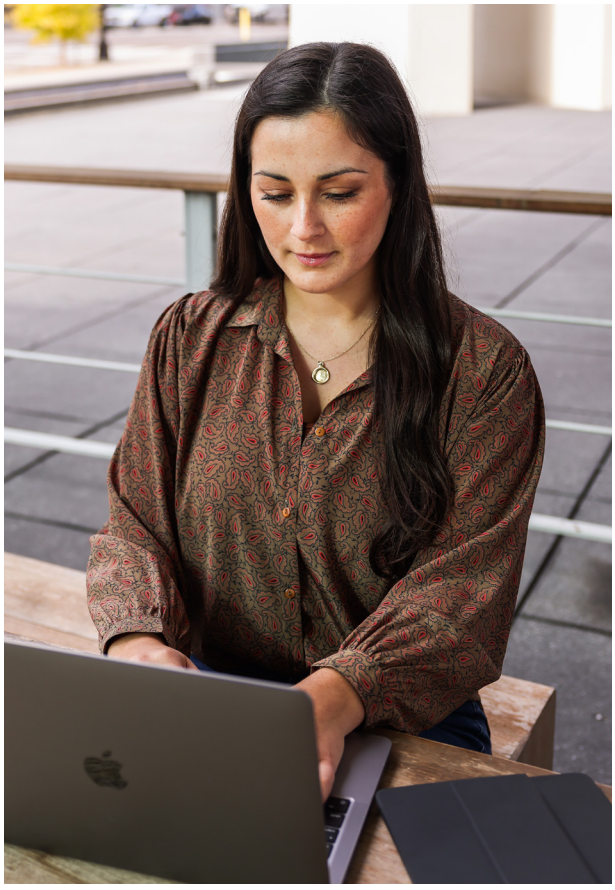
Stage four, resolution, is aptly named because it is here where IT/Security teams deploy remediation workflows to remedy vulnerabilities detected in the previous stages, working from the highest severity level to the lowest during this mitigation phase.

Last but highly significant to the vulnerability management process is reporting. During this phase, teams:

- Document all their findings (i.e., what happened).
- Annotate positive and negative outcomes (i.e., what worked, what didn't).
- Provide feedback to inform current and future workflows (i.e., the root cause of why something didn't work or what issues, if any, were encountered).
- Improve processes by reviewing lessons learned (i.e., things to be mindful of and what would make this better/easier/less error-prone in the future).

As part of a defense-in-depth strategy, EDR is able to achieve cyber success by securely integrating multiple solutions to:

- Actively monitor endpoints for multiple risks, alerting teams of detected issues, like malware or non-compliance.
- Analyze telemetry data, manually or using AI to identify both known and unknown threats.
- Automate threat prevention or quarantine affected devices until further review.
- Mitigate threats by sanitizing affected endpoints and automatically triggering remediation workflows.
- Proactive defense against threats, leveraging machine learning (ML) to perform threat hunting by quickly gathering and analyzing threat intelligence. Also, reducing response times and advising teams on how to respond.



7. AI-driven threat intelligence

AI and ML-driven solutions help teams of all sizes – not just those with dedicated IT/Sec pros – gather, analyze and make data-driven decisions faster than is possible through manual processes. And time is just the tip of the iceberg, as it were when it comes to the savings and ROI AI/ML yields organizations.

According to IBM, "AI improves its knowledge to "understand" cybersecurity threats and cyber risk by consuming billions of data artifacts." This is the core component that enables organizations to glean the following benefits from introducing AI/ML into their cybersecurity plan to:

- Work alongside administrators to get you the data you need to make informed decisions regarding threats based on customized threat intelligence tailored to your unique environment.
- Monitor, identify, research, exploit, verify and remediate unknown threats 24x7x365, as well as develop threat models based on logical and empirical data points.
- Proactively identifying and stopping threats before they escalate can increase ROI and save money cleaning up after costly data breaches (and compliance-related aftermaths).
- Respond to incidents faster while speeding up resolution times, narrowing the window between when threats are detected and when remediation occurs.
- Harness ML and automated security workflows to empower your IT/Sec teams to focus on developing better technology experiences that help stakeholders work smarter, not harder.

8. Device compliance policies

A key component of compliance is the device configurations used to reduce the attack surface of hardware and the software running on the devices themselves. The concept of hardening exists to effectively "lockdown" endpoints, getting rid of whatever isn't unnecessary for users to perform the tasks in their roles. Less code running = a reduction in risk vectors that can be exploited.

Frameworks are excellent guidelines for organizations to follow to maximize the security of their devices, data, services, processes and workflows. Yet, once configured, external factors, such as updates, malware, newly installed apps and risky user behaviors, can trigger modifications to existing settings to bring devices out of compliance.

If configuring settings is one-half of a security solution to compliance, then enforcement – performed by policies set up in your MDM, identity and security solutions – is the other half.

Several ways in which policies support an organization's security posture are:

- Enforce compliance baselines, keeping devices compliant with industry regulatory requirements.
- Ensure devices are using the latest version of macOS or productivity apps are up to date to prevent known vulnerabilities.
- Require Identity Provider (IdP) and security solutions to verify credential and/or device health data each time users request access to protected resources, preventing access to compromised accounts and remediating devices that do not meet security baselines.
- Maintain parity with organizational security baselines on BYO devices by automatically segmenting sensitive data and apps to a separate business volume upon enrollment while personal data and apps remain private.
- Force encryption on all wired and wireless connections when remote users connect to untrusted networks, ensuring data security.

9. Security awareness training

No comprehensive cybersecurity strategy is complete without a security awareness training program for end users.

According to Forbes, “93% of organizations had two or more identity-related breaches in the past year.” Pair this with a finding by Statista that placed the number of unique phishing sites detected worldwide in the 1st quarter of 2024 alone at 963,994. This crystalizes the belief that threat actors are targeting and capitalizing on users’ lack of security knowledge to compromise identities to further extend an attack’s reach.

The endgame in cybersecurity is to reduce the level of risk that impacts your company so that it is as minimal as your risk appetite can tolerate. With this in mind, security training acts as a complimentary component of your overarching security strategy to:

- Keep users informed as to the latest threats impacting your organization.
- Make common threats more identifiable so that users are less likely to fall prey to them.
- Minimize errors by strengthening the weakest link in the security chain: humans.
- Empower users to do their part in safeguarding devices and protecting sensitive information by limiting data leaks.
- Improve compliance holistically by ensuring users understand what is expected of them and that organizations adhere to strict accountability guidelines outlined in their policies.

10. Incident response plans

We've covered best practices that can work independently of one another but when combined, the layering of each security control, process and workflow evolves your security plan into a robust, more comprehensive strategy that catches threats before they can be exploited.

But what happens if a device still becomes compromised? That is where a solid incident response plan, one that integrates within your cybersecurity strategy, is a crucial element in mitigating threats as quickly as possible, according to the National Institute of Standards and Technology (NIST).

At a basic level, there are four steps to an incident response plan:

1. Preparation

- Align hardware/software configurations with security baselines to minimize the risk of non-compliance (data encryption).
- Integrate MDM and endpoint security solutions to simplify risk assessments and streamline vulnerability management with an up-to-date inventory (vulnerability assessment).

2. Detection and analysis

- Collect rich forensic data to paint a complete picture of what happened and, just as importantly, how the incident happened (EDR).
- Reduce data collection and analysis time from days or weeks to minutes by automating redundant security tasks with AI/ML technologies (AI-driven threat intelligence).

3. Containment, eradication and recovery

- Minimize risk factors and quickly resolve incidents with orchestrated remediation workflows by securely sharing telemetry data between MDM and endpoint security (regular patching and updates).
- Requiring additional factors for authentication provides a digital safety net that keeps data out of threat actors' hands if credentials are compromised (MFA).
- Keep users safe and productive from any device they work on, personal or institutionally owned, and consistently enforce security across your infrastructure on macOS, iOS/iPadOS, tvOS, watchOS, visionOS, Windows and Android devices (zero-trust architecture).

4. Post-incident activity

- Deploy device hardening configurations to enforce compliance through policy-based management workflows for easy, effective compliance management (device compliance policies).
- Minimize threat exposure through education and periodic awareness training to reinforce the information users can rely upon to spot common attacks, like phishing (security awareness training).

Conclusion

The time to test your backup plans is not when you're trying to recover data after a disaster. The same is true for cybersecurity plans.

Whether you're an SMB running everything from Apple devices to educational institutions that deploy 1:1 iPad programs for safe, private learning or Fortune 500 enterprises with thousands of users and even more devices running a combination of macOS/iOS, Windows and Android operating systems – there's no better time than now to fulfill your organizational security needs by implementing a comprehensive, defense-in-depth strategy to keep devices, users and data safe from growing, sophisticated threats and the bad actors whose aim it is to steal your organization's sensitive and confidential information.

jamf

www.jamf.com

Get started with Jamf

or contact your preferred reseller to get started