jamf

Crisis Control

Closing security gaps with incident response and recovery

"Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources."

The excerpt from the National Institute of Standards and Technology (NIST) emphasizes the need for a solid plan in addressing security incidents. A swift, focused response helps control risks by limiting potential exposure. The remediation phase, determined by available tools, varies widely.

Gaps happen.

In this paper, we address:

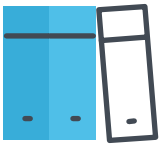
- What the five steps of incident response—preparation, detection, reporting, response and remediation—can teach us about building more robust security strategies to handle and remediate threats efficiently
- How to develop effective, robust playbooks to handle incident response for varied threats
- Why understanding the value of assets and assessing the potentiality of threats is paramount to successfully responding to and recovering from security threats
- Why an integrated approach to management and security, with a purpose-built security solution, is the way to secure your Apple fleet

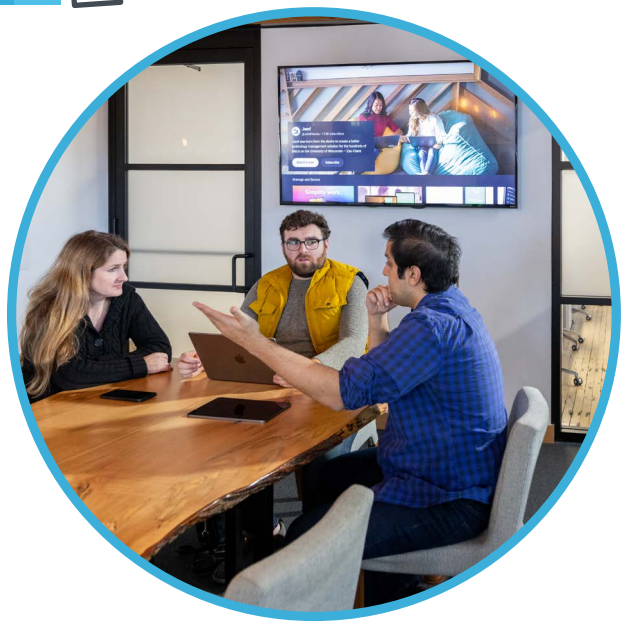
I. Preparation

Set up your environment for success.

Benjamin Franklin's saying, "An ounce of prevention is worth a pound of cure," rings as true today as it did when spoken. And it could not be a more fitting message for IT—specifically, protection against cybersecurity threats and attacks.

Proper policies, people and tools are critical for successfully mitigating incidents and remediating any affected devices promptly and efficiently. Doing so also cuts down the potential of a threat to compromise system processes or diminish business continuity in meaningful ways.





Inventory

How can something be protected if no one knows it exists? Therefore, it is crucial to maintain up-to-date inventory management to protect all assets. It is a good practice for organizations to keep tabs on:

- What equipment, peripherals and resources do they own?
- How are they configured?
- Where are they located?
- Who are they assigned to?
- Which access permissions are granted and to whom?

The answers to these questions provide organizations with essential information directly relating to the security of devices and resources used for work.

Identifying and inventorying equipment and their respective uses provides an accurate picture of what equipment the organization owns and what it is used for. Be sure to include any valuable services these devices may provide, such as identifying public-facing servers that serve web content, mobile devices used in telehealth that store medical records or private patient data, etc.

Risk assessment

After inventory, the next phase is assessing risk factors:

- Determining what threats the devices are susceptible to
- The probability that the threat will be exploited
- What the potential fallout may be
- How that ties back to and affects the organization’s business continuity plan

Assessing risk factors is a complex task that demands a wealth of information to depict the organization's devices and resources accurately. It requires a deep understanding of technical, security, financial, administrative and legal aspects to evaluate devices and their services correctly. Risk assessment isn't done in isolation; it involves multiple stakeholders considering various product or service evaluations before reaching a final decision.

Consider a web server as an example. Web servers are publicly accessible and aremore vulnerable than devices protected behind firewalls. If a web server connects to a database storing user information, the risk increases as it becomes a gateway to personally identifiable or confidential data.

Standards and regulations

Understanding the organization's assets and having a plan for incident response are distinct yet interconnected aspects.

In the event of computer security incidents, a well-defined playbook becomes crucial for response protocols, enabling Computer Security Incident Response Teams (CSIRTs) to act promptly, regardless of team size or external partnerships. The clear and concise plan aims to:

1. Align organizational resources with industry laws or regulations, establishing compliance baselines.

2. Efficiently address detected threats before they escalate, providing the fastest route back to a compliant status.

While policies may vary, NIST outlines key elements for developing organizational incident response policies, including a commitment statement, policy purpose, scope, definitions, organizational structure, risk assessment, performance metrics and reporting procedures.

Incident response processes

Some elements govern how to respond to incidents, and others address the incident response plan, which details the stakeholders and the respective steps to respond to an incident.

Remember, everyone has a role to play – regardless of whether it is hands-on or calling the shots behind the scenes – it is most certainly a team effort. The plan itself serves as the roadmap with a focused and coordinated approach to responding to incidents based on the organization's unique requirements while leveraging its capabilities and partnerships for maximum effectiveness.

Like the policies above, the plan can and will vary based on the organization's mission, size, structure and functions.

Key elements to consider when developing a successful plan include:

- Mission statement
- Strategies and/or goals
- Organizational approach
- Approved communication processes
- Metrics measuring effectiveness
- Process for optimizing capabilities
- Integration into the organization’s processes

Administrative considerations

At this point, the organization should either have a team in place or a clear idea of suitable individuals and their roles in the incident response model, synthesizing information from earlier sections. For instance, IT and Information Security department members are ideal for the response team due to their extensive infrastructure knowledge. Additionally, individuals with project management experience are vital in expediting the remediation process by efficiently organizing and scheduling necessary resources. The approach varies, with larger organizations usually having dedicated internal teams for handling security concerns, while smaller ones are encouraged to collaborate with external providers for incident response support, leveraging their unique strengths as needed.

Establishing partnerships isn't limited to smaller organizations; larger, dedicated teams often collaborate with vendors, law enforcement and entities like the United States Computer Emergency Readiness Team (US-CERT) in the U.S., coordinating incident response activities. Vendor partnerships can offer beneficial services, and companies must be familiar with the governmental organization overseeing incident response in their country or region for additional support. This is especially vital when organizations lack specific expertise or face severe incidents like large-scale attacks, where partnerships with ISPs can help mitigate threats like DDoS attacks.

Creating response teams involves answering key questions to tailor the team to the organization's unique needs:

- Will the team function best as a centralized model or distributed across multiple locations?
- Who will coordinate among internal and external teams, including entities like US-CERT?
- How do industry regulations impact the type(s) of incident response support the organization can develop or partner with?
- Is there sufficient internal staff for prompt incident management, or is partial/full outsourcing needed?
- What are the incident response team's availability requirements, considering 24x7x365 on-call rotations and full-time vs. part-time support?
- What budget considerations are necessary to fund the team, covering salaries, PTO, skills gaps and continuing education?
- For smaller organizations, what options exist to protect assets when dedicated teams aren't feasible, and what planning is needed for a quick response when necessary?

This information becomes an invaluable tool that shapes decisions regarding the types of security devices required, including procuring services to ensure they are fully protected. Not all solutions perform the same functions, so why would a generic solution be the right fit for such dynamic technologies? **The answer is that often, as in the case of Apple products, generic solutions are not the best fit since they do not offer the comprehensive coverage and insight that purpose-built products, like Jamf Protect — our purpose-built Apple endpoint security solution — offer.**

II: Detection and reporting

Identify threats

> “If you only have a hammer, everything looks like a nail.”
>
> **- Benjamin Franklin**

This quote refers to the **law of the instrument**, a cognitive bias that involves an over-reliance on a familiar tool and may lead to seeing only part of the picture. When viewed solely through an InfoSec lens, the relation to the security posture of the devices owned by your organization presents an obstructed view that becomes a severe problem when information critical to the health of your devices is not visible. This lack of insight into device health further complicates matters, potentially leading to even greater repercussions and negatively impacting the organization’s security posture because a threat or vulnerability was not visible.

Visibility is key to appropriately actionable responses. And there are the two key phases where the proper tooling — combined with up-to-date data — can and will make all the difference between resolving an issue quickly or not:

1. Before the alert is raised

2. During the remediation phase itself

Alerting and notifications

Before receiving an alert, it needs to be triggered. Ideally, the organization's tools should offer alerting capabilities by actively monitoring endpoints through various methods, not just relying on signature-based approaches for known malware. In addition, a robust process using heuristics or analytics can detect potential malware and other threats, including risky actions or unusual employee behavior based on patterns.

Behavioral analytics are useful for alerting teams to potential threats from unknown malware variants that may not have a detection definition available. This system allows IT to prioritize indicators once an anomaly is detected. During the investigation, team members must confirm the accuracy of detections to identify false or true positives. Confirming false positives saves time and organizational resources while verifying true positives allows the dispatch of appropriate resources to prevent threats from growing and causing broader impacts or potential data breaches.

Stream logging data to SIEM

These logs are not just for showing or troubleshooting app crashes—they provide valuable information on system and app processes. While diving into a sea of logs might seem counterproductive during a cybersecurity incident, the key is centralizing, organizing and analyzing specific security-related data, drawing key insights to the foreground.

Starting with log collection, an organization's sheer number of devices can be overwhelming. Add the challenges of accessing logs from distributed workforces, and the task becomes even more daunting. Manual sorting and analyzing relevant data from logs can take hours or involve large teams.

Enter SIEM (Security Information and Event Management). SIEM plays a crucial role in your organization's security processes by:

- Identifying current security threats affecting endpoints.
- Assisting teams in responding to and triaging incidents swiftly, allowing your teams to remediate and resolve security incidents.
- Verify and ensure compliance with standards and regulations.

SIEM quickly analyzes logs from all endpoints, offering insights into the operational, functional, technical and security status of apps and data within the endpoint. It answers questions such as:

- What are a device's patch levels?
- Which actions were performed by the system?
- When were processes executed?
- Where was the device communicating from?
- Why did the device, app or thread behave a certain way?
- Who carried out a particular task or action?
- How was this vulnerability exploited?

III. Triage and analysis

Analyze threats

Before simply acting on every potential threat identified, it's important to assess, to assess the possibility of false positives or issues getting misdiagnosed.

The central purpose of triage and analysis is:

- Investigate the issue detected or reported
- Prioritize security events based on severity
- Allocate resources necessary to analyze data
- Determine the validity of a threat or attack

Streamlining analysis with SIEM

Your SIEM solution collected log data so that your IT and Security teams can use it to granularly analyze sorted data before taking precise action(s) to mitigate threats and remediate issues with minimal resource expenditure. Or better still, **extend SIEM functionality** by integrating it with their MDM and/or Endpoint Security solutions to **visualize critical information security data points** and execute automated remediation workflows the moment threats are identified for even faster incident response and clean-up.

Preventing known threats

Incident response aims to address identified threats, but proactive prevention of known threats is more crucial than reacting to an attack. A comprehensive incident response plan incorporates diverse tools and features to prevent cybersecurity issues from multiple perspectives. A defense-in-depth strategy, which prepares you to catch threats through various layers of defense before you fall victim to them, does not rely on a single approach.

One key layer in defense is analytics, aligned with **the MITRE ATT&CK framework,** a repository of real-world adversary tactics and techniques. This global knowledge base fosters collaboration among organizations, developers, InfoSec professionals and the security community to enhance cybersecurity practices, minimize risk, and maximize threat defense.

Integrating this functionality into your endpoint security solution protects devices accessing organizational resources from risks posed by known threats and their attack vectors. MITRE ATT&CK **maps each threat to an analytic within your endpoint security solution**, taking action to block or quarantine threats during active monitoring.

These analytics cover desktop operating systems and address modern threats, including those targeting mobile devices for enterprise and personal use. This holistic approach includes threat prevention for mobile threat defense (MTD) alongside desktop OS security. In cases of complex threats or those converging with others to evade detection, analytics collaborates with device management solutions for advanced Security Orchestration, Automation, and Response (SOAR)-like workflows. In situations requiring intervention, data and analytics direct the incident response team response, like limiting network connectivity, containing the infection to the affected endpoint and preventing threats from spreading across the organizational network.

Hunting unknown threats

Integrating SIEM technology with endpoint security provides security teams with advanced capabilities for threat-hunting analysis. When you combine rich telemetry from endpoint security products and a SIEM with the expertise of your security team, researchers can delve into system processes, using the latest telemetry and logging data in one console to hunt for, identify and address potential unknown threats.

Dedicated threat-hunting teams, like **Jamf Threat Labs (JTL)**, continuously research and update endpoint security rules to keep endpoints protected against the latest threats. If your organization lacks a threat-hunting team, especially for medium to larger organizations, choosing a product that already commits significant threat-hunting resources to maintain cutting-edge endpoint security is highly recommended due to the rapidly changing tactics of threat actors and the emergence of new, unknown threats.

Smaller organizations without the resources for an in-house team are encouraged to partner with service providers to establish a threat-hunting team. This collaboration aids in proactively identifying potential threats that may have gone unnoticed or are generally unknown, safeguarding the organization from data harvesting while evading detection.

IV. Containment and neutralization

Response and remediation

The incident response process involves monitoring, detection, investigation, and remediation. Remediation addresses issues identified as real, using a different set of tools to correct problems and return affected devices to their normal state. The effectiveness of incident response and remediation depends on factors unique to each organization, such as risk factors, skill sets, security tools, partnerships, policies, regulations, security plans and budget.

Endpoint management tools should offer robust support for the devices they manage. In an Apple-centric environment, lacking support for the latest Apple security and device management frameworks can hinder the organization's ability to respond quickly to threats. Comprehensive support aligns with the organization's IT/security policies, reducing stress on teams during incidents or change management projects.

Having the right tools is crucial, as delays, inadequate reporting, or inefficient remediation can lead to costly consequences. Seamless integration, working in the background to protect devices and swiftly remediate issues, relies on processes working harmoniously with purpose-built technologies, such as Jamf solutions for Apple infrastructure. These solutions ensure security, optimal performance, compliance, and immediate support with the latest features.

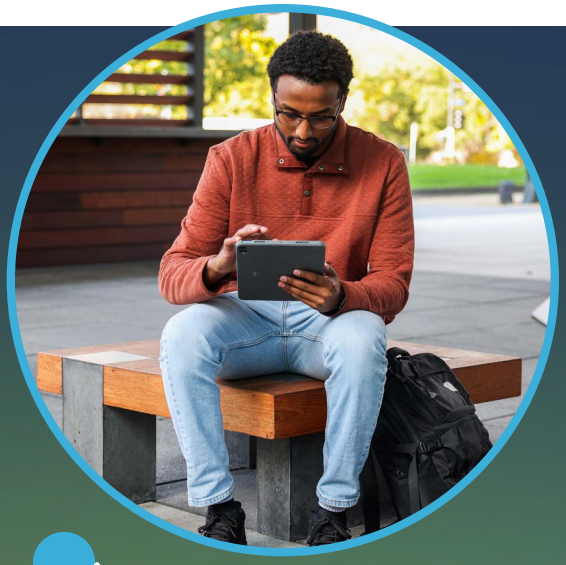
Advanced workflows to further secure your environment and aid in incident response and remediation.

Device provisioning

Deploying new devices to users or provisioning access to user's personal devices used for work adds a dimension of risk. Did users configure their personal devices properly? How can IT verify that security solutions are enabled on endpoints? What can be done to limit risk exposure on compromised devices?

The answers to these questions are provided through provisioning workflows tied to centrally managed account credentials as part of an **Identity and access management (IAM) solution:** one that reaches from the initial deployment of the device throughout the entire device lifecycle. By relying on IAM, access permissions are intrinsically bound to the user's credentials — granting only the necessary permissions to the resources with just-in-time provisioning providing access when needed.

Moreover, provisioning through zero-touch deployment workflows provides first-level, foundational support for incident response tasks and remediation workflows, not only **ensuring that endpoints are set up correctly from the start** — but that in the event of an incident — additional protections can be layered atop to mitigate risks from threats while minimizing the fallout from attacks to speed up recovery processes.



Identity and access

Identity and access management (IAM) goes beyond just accounts and passwords to secure the exchange of sensitive data. It has evolved into its own **comprehensive identity-based security solution**, which effectively protects resources from the modern-day threat landscape through multiple workflows beyond merely connecting users securely to organizational resources or requiring them to set a strong password.

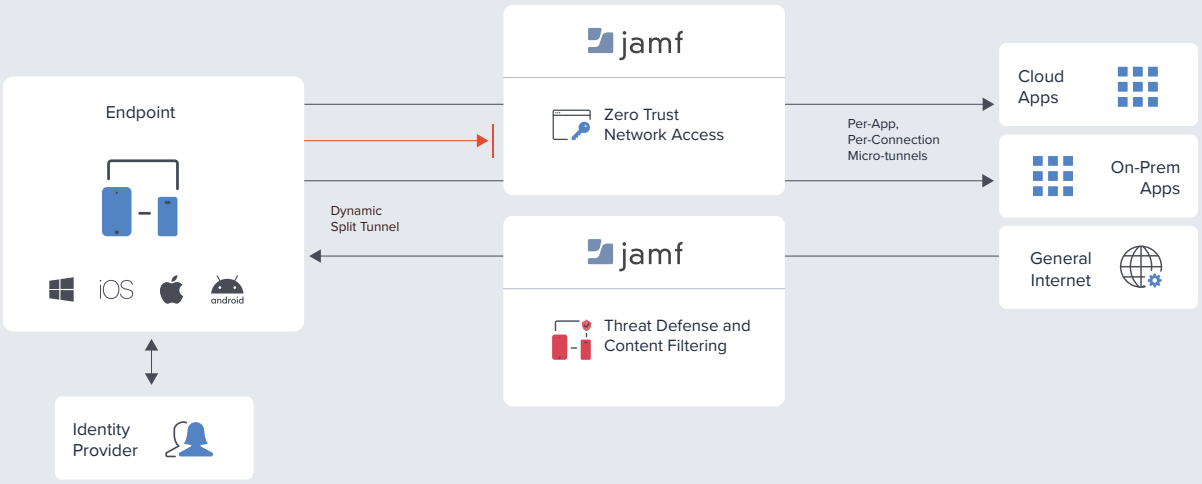
Policy enforcement

Policy-based management is essential for maintaining a device's security posture according to an accepted baseline. Various factors impact the security posture, like:

- App updates
- New OS versions
- Security patches
- Evolving organizational requirements
- User behaviors
- Emerging threats

Policies representing minimum rule sets help maintain a known level of security despite the unpredictable nature of these factors.

Zero Trust Network Access (ZTNA) technology utilizes a policy-based enforcement framework. Devices and users undergo risk assessment when requesting access to a protected resource. In a zero-trust approach, access is initially denied and must be granted based on organizational criteria. Access remains denied if a device or user fails to meet these criteria



Secure network connections

To effectively deal with modern threats, we need modern technologies. VPN, a legacy technology that has secured network connections for decades through encryption and user credentials, falls short in meeting the needs of today's computing environments and the evolved threat landscape. VPN lacks scalability, adherence to the principle of least privilege, compensating controls for lateral movement attacks, risk assessment based on device and user health, and integration with centralized identity solutions.

In contrast, ZTNA secures network connections like legacy VPN solutions but without their drawbacks. ZTNA is designed to offer security workflows that integrate with modern solutions, ensuring compatibility with various device types across the entire infrastructure. It eliminates the administrative challenges of maintaining complex configurations and avoids the financial burden of managing legacy VPN hardware.

Device management

Mobile Device Management (MDM) is more than a “nice to have” when it comes to addressing issues that impact security. From an individual endpoint to scaling across your entire fleet, it’s a requirement to maintain your organization’s overall security posture. It plays a crucial role as it is woven directly into the fabric that makes up a holistic approach to safeguarding devices against threats. Similarly, endpoint security solutions share a relationship with device management. You cannot thoroughly verify something is secure if it’s not managed, nor can something be fully managed if it’s not secure.

Examples of management capabilities that further secure your environment while aiding in incident response and remediation are:

Inventory

Maintaining an up-to-date inventory of devices is crucial for various aspects, including tracking device status, identifying potential risk factors and ensuring that the right people have the right tools for their jobs. Inventory management goes beyond tracking equipment and is key in ensuring that users, their devices, and organizational data are always accessible and under control.

A mature IT Asset Management (ITAM) program provides valuable insights for your organization's holistic security plan:

1. Critical device information

- Hardware details: device types, models, and serial numbers
- Software information: OS version, installed apps and their versions
- Security configurations: managed settings, hardening profiles and encryption status
- Management details: enrollment methods, warranty information and managed/ supervised statuses

2. Foundation for risk assessment

- Enables risk assessment and quantification processes, informing the development of comprehensive security strategies.

3. Actionable data

- Converts inventory data into actionable insights, guiding next steps and iterative IT-related tasks.

4. Support for security teams

- Provides up-to-date device information to Security teams, assisting in incident triage, response, and efficient remediation workflows when combined with baseline data.

Automation

Automating processes is more than relying on technology to make the admin's role a bit easier. Sure, the ability to simplify, in this case, the deployment of managed apps, secure configuration profiles, or patch management helps ease the burden on IT relating to a few of the common administrative tasks they perform regularly and en mass.

However, the key benefit of automation is that it minimizes the chance that human error might introduce unintended effects that could otherwise impact the efficacy of your security plan.

Some of the ways automation can make — or break — a security posture are:

Make	Break
App Installers deploy and update apps, ensuring the latest version is always installed to minimize vulnerabilities.	Different versions of apps are installed, some updated, some not.
Configuration profiles are managed, scoped and deployed via your MDM solution — no user interaction is necessary.	Admins rely on end users to set appropriate device configurations.
Standardized workflow configures encryption, enabling encryption and a recovery key escrowed safely.	Volume encryption is recommended to keep data safe.
Warranty information is populated and kept track of from the date of purchase.	A damaged device requires a service call to the vendor for repair support.
Zero-touch deployment ensures that company-owned devices are ready for management and use from the moment the device is powered on.	Users are responsible for enrolling company-owned devices in the organization's MDM.
Organizations can track missing devices, lock and remotely wipe them using MDM commands, and ensure that data remains safe.	In the event of loss or theft, users are responsible for keeping data safe from unauthorized access.
Policy-based workflows execute updates according to organizational requirements to minimize risk from a vulnerable, outdated operating system (OS).	Users are responsible for keeping the system OS up to date.

Consider the following real-world scenario: A user's personal device uses an outdated OS. They have opted to postpone updating to the latest OS as long as possible because they rely daily on an app that the latest OS does not yet support. Despite the known security implications, they continue to use the vulnerable device for work alongside personal uses.

How can you automate the mitigation of this security threat and keep organizational data safe?

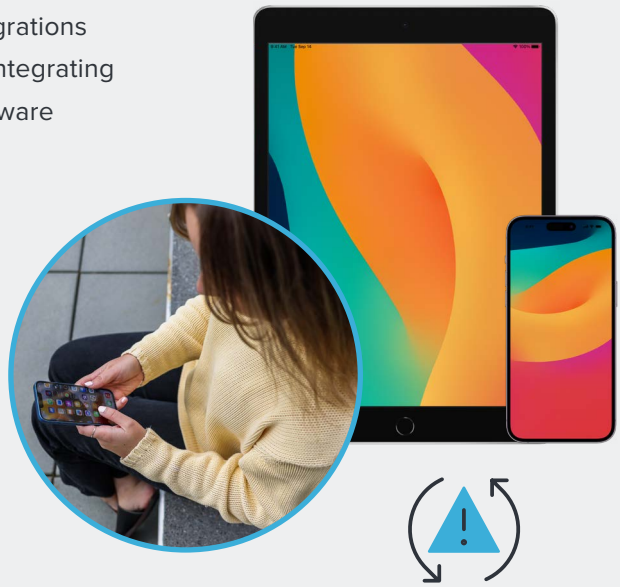
Integrating your MDM and Endpoint Security solutions enhances functionality for IT and Security teams, enabling advanced incident response and remediation workflows.

The endpoint security software checks the personal device's telemetry data against minimum requirements before granting access to sensitive company resources.

If the initial request is automatically denied for safety reasons, the device's telemetry data is securely shared with the MDM solution. MDM policies mandate that the device run the latest OS, triggering a remediation task to upgrade the OS.

After completing the task, the endpoint security solution re-scans the device to confirm threat mitigation. If successful, access to company resources is granted; if not, the request remains denied, and additional remediation steps may be needed.

Automation continues beyond this point. Similar to how integrations with IAM solutions expand identity and access capabilities, integrating between your **best-of-breed MDM solution** and various software extends functionality.



Never trust — always verify!

Endpoint security

In an ideal scenario, comprehensive endpoint protection safeguards all Apple computers and mobile devices from the modern threat landscape. However, real-world business is not exclusive to Apple hardware, and being Apple-best doesn't mean Apple-only.

Most environments are mixed platforms, so comprehensive endpoint protection must extend support beyond the Apple ecosystem to Windows and Android endpoints for effective protection against new and evolving threats. This holistic approach ensures efficient defense-in-depth strategies covering various device types and operating system (OS) architectures.

Since no OS is immune to threats, security solutions with powerful and flexible workflows help organizations succeed with Apple and other mobile devices. These solutions prioritize data security, user privacy and end-user productivity.

Endpoint security capabilities—including mobile threat defense and vulnerability management— combine to manage and secure devices throughout their entire lifecycle.

Mobile Threat Defense

Securing data can be challenging, especially for organizations with distributed workforces. The difficulty increases when there's a lack of integration between management and security tools, coupled with evolving threat tactics. This situation makes it tough for InfoSec professionals to respond quickly and efficiently to threats.

Mobile threats contribute to these challenges because they represent a new frontier for security incidents. With an estimated 6.7 billion smartphone users globally, work is increasingly happening on mobile devices, which naturally leads to threat actors focusing their attacks on mobile endpoints (Statista 2023 forecasts). Mobile devices encompass smartphones, laptops, tablets, wearables and even some IoT devices, introducing multiple operating systems like Apple, Windows, Android, and Google Chromebooks.

Mobile devices pose a significant risk, emphasizing the need for a comprehensive security solution, one that prioritizes protecting organizational resources by aligning security controls to prevent mobile device threats as effectively as threats on other devices across the enterprise.

Vulnerability management

According to NIST, the Common Vulnerabilities and Exposures (CVE) system is a list of entries that includes an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities. It helps identify, describe and reference vulnerabilities in computing code.

But determining OS or app vulnerabilities in your environment often relies on separate vulnerability assessment software. This software, used by pen testers, detects threats and classifies them based on severity levels.

Using a standalone vulnerability assessment tool requires more resources than directly integrating this feature into your preferred endpoint security solution. Integration makes it essential to your InfoSec team's workflow for threat prevention, incident response and remediation to mitigate risk and maintain compliance.

Integrating vulnerability management into Jamf Protect enhances incident response by allowing security professionals to prepare for and mitigate risks proactively. This approach is more proactive than waiting for an app or OS to be exploited before reacting to the incident.

Trusted Access

Three security paradigms — **one holistic platform.**

An end-to-end Apple-centric solution, that integrates device management, identity provisioning, secure connectivity and endpoint security into one comprehensive, holistic and centralized platform.

...but one that is flexible enough to extend in-network and layered security protections while streamlining incident response and remediation workflows for supported platforms.

Management	Identity	Security
• Keep endpoints and apps up to date with patches • Ensure optimal performance without compromising **security** or **privacy** • Automate remediation of security threats to reduce risk • Maximize **layered security protections**/defense in depth	• Maintain compliance through **context-aware** policies • Provision cloud-based identities and centralize password management • Secure remote connections with next-generation **ZTNA** technology • Implement **Multifactor Authentication** (MFA) workflows for an added layer of access security	• Monitor systems processes and prevent malware threats • Analyze endpoint health frequently to mitigate baseline shifts • Obtain rich telemetry data to inform IT and Security team decisions • Advanced **machine learning** (ML) and **threat intelligence** engine (MI:RIAM) drive **threat hunting** and prevention — on-device and in-network

Compliance alignment

Maintaining compliance is crucial given the constant threats and novel attacks reported by the media, putting pressure on IT and security teams. With regulations in play, ensuring every device, user or piece of data remains compliant becomes a significant challenge.

An example: Mobile devices on iOS 17 on October 24, 2023, at 9:59 a.m. technically became non-compliant one minute later when iOS 17.1 became available. This illustrates that compliance is subjective and transient.

It's important to distinguish compliance from security protections. Compliance is a fleeting state, while security is a roadmap to reaching it. The intersection of compliance requirements and security controls often forms a framework guiding IT and Security teams to meet compliance goals.

Combining solutions empowers incident responders to enforce compliance through policy-based management workflows. This automation ensures devices are brought back into compliance after falling out, triggered by alerts like missing apps or misconfigurations following an OS update.

V. Post-incident activity

Informing future processes and practices

Document findings

Record all findings, regardless of size or significance. Documentation informs stakeholders about issue causes and resolutions. It fosters collaboration for developing better solutions and optimizing incident response, remediation workflows, and policies.

Lessons learned

Documentation goes beyond recording events; it provides valuable insights. Regular review of findings enhances the incident response and remediation process. It leads to greater efficacy, eliminating unnecessary steps and improving overall value.

Continuous monitoring

View processes as cyclical, not linear. After implementing a workflow, bring findings back to stakeholders for review. This iterative approach allows analysis, comparison to baselines, and adaptation to changes in technology and processes. It aims to reduce risk, minimize impacts, and improve efficiency significantly.

Training

The goal is to create better, streamlined workflows that optimize security efforts. This involves aligning response and remediation plans with IT and Security teams' missions. The focus is on addressing unique organizational and user needs while minimizing downtime.

Summary

If you’re ready to take the next step in creating or strengthening your incident response and remediation plan, Jamf can help.

Try us for free to see how it's made possible, or contact your preferred reseller to get started.