jamf

WHITE PAPER

The Guide to Successful macOS Security Incident Response

When a cyberattack or security breach occurs, how efficiently and effectively an organization reacts is directly correlated to the amount of damage incurred and recovery time and cost lost. This process is referred to as security incident response and is a critical component of any successful security program put forth by IT or Information Security teams.

While most organizations have a robust practice to defend against security threats, there are tools, workflows and best practices to ensure your organization is prepared and ready should a cyberattack or security breach take place. And with Mac numbers in the enterprise on the rise, now is the time to enhance your Mac security practices and ensure your organization is protected.

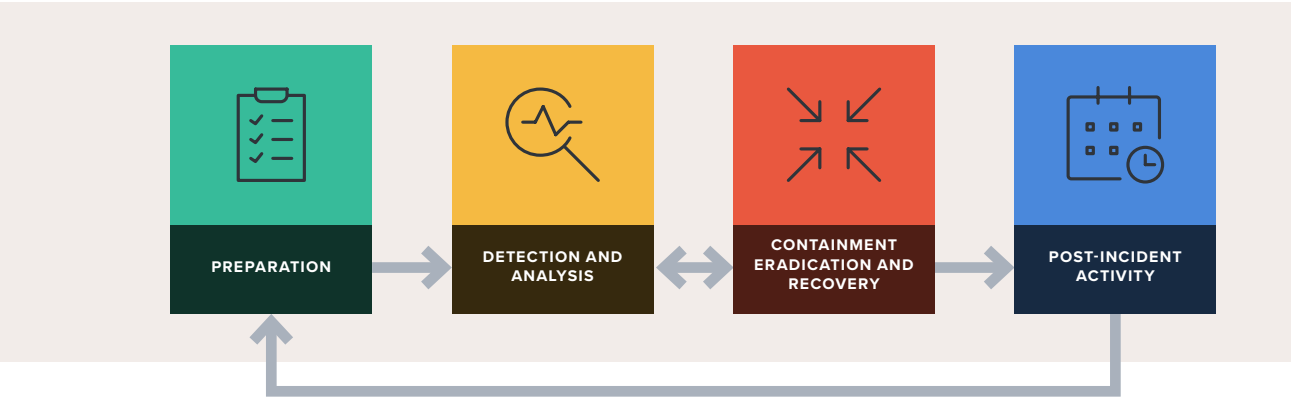
In our white paper, you'll learn steps to:

1. Prepare for incidents
2. Detect and analyze incidents
3. Contain, eradicate and recover from incidents
4. Monitor post-incident activity

Unique attacks require unique defense

As Mac adoption rises, additional attention is needed within organizations to protect and secure Macs beyond what Windows-centric security solutions provide. Mac has always come with built-in security tools, but new modes of attack and a larger market share demand better methods to protect the operating system and organizational data. But regardless of how you leverage your Mac security solutions, incident response should be methodical and consistent.

As set forth by the National Institute of Standards and Technology (NIST), the four components of a security incident response are:



Step 1: Prepare for incidents

Security is a top priority for almost every organization, and with the shift to a larger remote workforce, it will be even more important. IT admins need endpoints to be as secure as possible. Endpoints must be managed, monitored, patched and configured for security. To do this, a variety of tools come into play.

Jamf Pro provides dashboards that keep you appraised of the state of Mac devices and flags hardware that needs attention. Through patented Smart Group functionality, IT admins can target devices that need to be updated, reconfigured or patched to improve their security posture. This is all done remotely and can be automated without IT physically touching the device.

To ensure visibility of what's happening on a device, Jamf Protect — enterprise endpoint protection purpose-built for Mac — gathers process and file information along with other behavioral analysis; all of which are helpful to be used for real-time and post analysis to identify malicious activity and generate alerts. Important things to note:

- Jamf Protect's threat prevention will automatically block and quarantine malware and adware. Organizations that want to limit specific unwanted software can also define that within Jamf Protect through signatures, developer TeamIDs, etc.
- Common attack patterns against macOS are detected through analytics built into Jamf Protect. To ensure that the detection mechanisms mitigate risks correctly, analytics are mapped to MITRE ATT&CK® Framework and provide reliable coverage against attack vectors.
- Jamf Protect collects a robust level of data associated with any identified attack, so you can see all processes, users, groups and binary information when a threat is detected.
- Data and alerts can be sent from Jamf Protect to your SIEM. Additionally, log data from the macOS Unified Logging can be sent directly to your SIEM or other system of record.
- Many attacks have common responses that can be configured and automated for your desired response and remediation actions with Jamf Pro.
- Additional response workflows can be triggered automatically or manually executed during an incident response in Jamf Pro using scoping to Smart Groups to push policies and configuration profiles.

Policies and configuration profiles allow for:

NETWORK ISOLATION	Isolate devices that may be under active attack where the damage needs to be contained.
PENALTY BOX	Restrict an untrusted user from corporate resources.
LOCK DEVICES	Lock users out of a device while you investigate suspicious activity.
DELETE OBJECTS	Remove unwanted applications, plugins or files from the device remotely.
QUARANTINE DEVICES	If an incident requires physical access to a device and is unable to be recovered remotely, quarantine and isolate the device until IT has physical control.
RUN CUSTOM SCRIPTS/COMMANDS	Leverage scripts and commands to remotely recover data or device information without physically touching the device.
CUSTOM END-USER MESSAGING	Communicate information like attack attempts made or organizational policies and best practices directly to end users.
RECOVER DEVICES	Remotely redeploy macOS and applications to a device that needs to be returned to a clean slate.

Step 2: Detection and analysis

Even with the security team in a position to be alerted in the event of an attack indication, they should still not become complacent. Despite the preparation and preventative mechanisms in place, security teams should assume that attacks will get past their best defenses and be ready to engage.

Imagine an end user accidentally downloads a compromised application...It's time for your endpoint security solution to get to work. When the security incident occurs, and you have no idea what the impact is, you need to collect the relevant information, analyze the threat and have ability to isolate that device to deter further contamination.

Security teams always need more visibility during an incident investigation and they often collect logs from a variety of systems and devices in SIEMs or other log aggregation systems in an attempt to achieve that visibility. When an investigation or audit is underway, an organization can then have a complete and customizable picture of what is happening on their fleet of Macs.

Step 3: Containment, eradication and recovery

When an attack is active in your network, time is of the essence. First, the attack has to be stopped and prevented from spreading to other systems. Because of your preparation, the relevant processes will likely be blocked by Jamf Protect, but that does not mean that other not-so-obvious attacker footholds are eradicated. To minimize the potential for damage when responding to an activity-based alert, Jamf Protect leverages Smart Group technology as well as all mobile device management (MDM) and Jamf Pro commands. Automated response examples include:

- Isolating the machine on the network so it can only talk with management infrastructure.
- Reducing access to cloud or corporate resources.
- Providing guidance to the end user that there is malicious activity on their device and to refrain from further actions.

Once the device is safe and the attack has been stopped, the IT and security teams will want to investigate further into what happened on the device and if there are any other scripts, binaries, backdoors, new credentials or any additional risks that persist. With Jamf, teams can:

- Retrieve blocked binaries from quarantine for inspection.
- Remove identified binaries or other files.
- Identify newly installed applications.
- Identify new local user accounts.

Once Jamf has mitigated an attack, devices still need to be brought back into a trusted state. With the power of Jamf Pro's policies and Smart Groups, you can clean up your environment without additional overhead by:.

- Running custom scripts / commands to reset security settings.
- Custom end-user messaging to direct them to additional help resources.
- Redeploying macOS on the device and reinstalling any applications.

Step 4: Post-incident activity

Jamf Protect delivers IT and security teams timely notifications when an incident may have occurred and provides the tools to analyze exactly what happened. While containment, eradication and recovery processes are often custom built in the Windows world, Jamf brings this functionality to Mac, so teams can respond and remediate in the way that best supports Apple the next time a security incident takes place.

After an incident:

- Jamf Protect continues to monitor and report on any additional threats and activity.
- Jamf Protect Analytics can be customized and expanded to cover additional targeted threats your IT or InfoSec team identify.
- Add identified threat binary information into a custom prevent list to ensure the entire Mac fleet is protect.
- Ensure that end users targeted by an attack are recertified on operational InfoSec education.

Better Mac security starts today

In order to effectively evaluate a security incident and determine the potential vulnerability from a breach, Jamf Pro paired with Jamf Protect enables you to monitor, prevent, detect and respond to the myriad of attacks that can wage against your Mac fleet.

From end users downloading compromised applications to spear phishing attempts or ransomware attacks, remediation allows you to take the necessary actions to secure your hardware, software and organization's data.

Put our security incident response features to the test with a free trial.

Request Trial Or contact your preferred reseller of Apple.