jamf

Mobile Threat Defense

for Beginners

It's a fact: Apple builds one of the strongest out-of-the-box secure platforms on the market. However, it is a growing platform target for determined attackers, and because of this, organizations must be equipped to respond to and fend off the threats of today and the future.

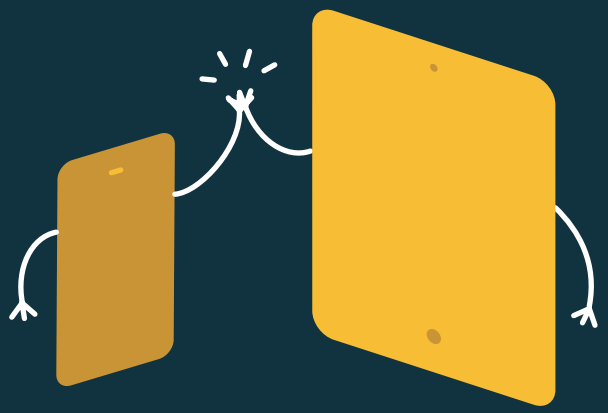
Common attack campaigns including phishing, malware and vulnerable apps are used to exploit devices and leverage access to company resources and sensitive data, such as:

- Exfiltration of confidential information
- Obtain access to corporate services
- Gather privacy data from users
- Intercept network communications

Jamf Threat Defense secures your mobile endpoints against compromise through threat detection and prevention of zero-day phishing and malware attacks. This is among the top concerns for all organizations, especially those that have adopted remote or hybrid environments, given the rise in targeted incidents against mobile devices from threat actors.

IN THIS GUIDE, WE'LL DISCUSS THE FOLLOWING:

- Comprehensive threat detection & prevention
- Strong protections for every use case
- Real-time reporting capabilities
- Policy controls and conditional access
- Unified operations management



APPLE IS A GROWING PLATFORM TARGET FOR DETERMINED ATTACKERS AND THEY DON'T DISCRIMINATE.

Organizations that deploy macOS devices to their users rely on Jamf Protect to provide endpoint protection to safeguard their fleet against security threats, preventing malware and providing insight into device health. But what about mobile devices, such as iOS and iPadOS-based devices? What kind of endpoint security is available for mobile devices that not only meet their unique needs, but integrate with Jamf Pro for an comprehensive management solution?

Enter **Jamf Threat Defense** — the purpose-built solution to protect Apple mobile devices and your users from malicious threats while maintaining a small footprint with minimal impact to device performance and the end-user experience.

“PROTECT YA NECK”

Harking back to the prolific words of the Wu-Tang Clan, the heading refers to essentially the protection of sensitive assets by protecting the core. For the purposes of this guide, the core is mobile devices. After all, they are the conduit by which attackers will target in order to access sensitive data.

41% of organizations experienced a malware incident on remote devices, which is not only a startling amount but also a sizable increase from the prior year, according to the **Cloud Security Report 2021**.

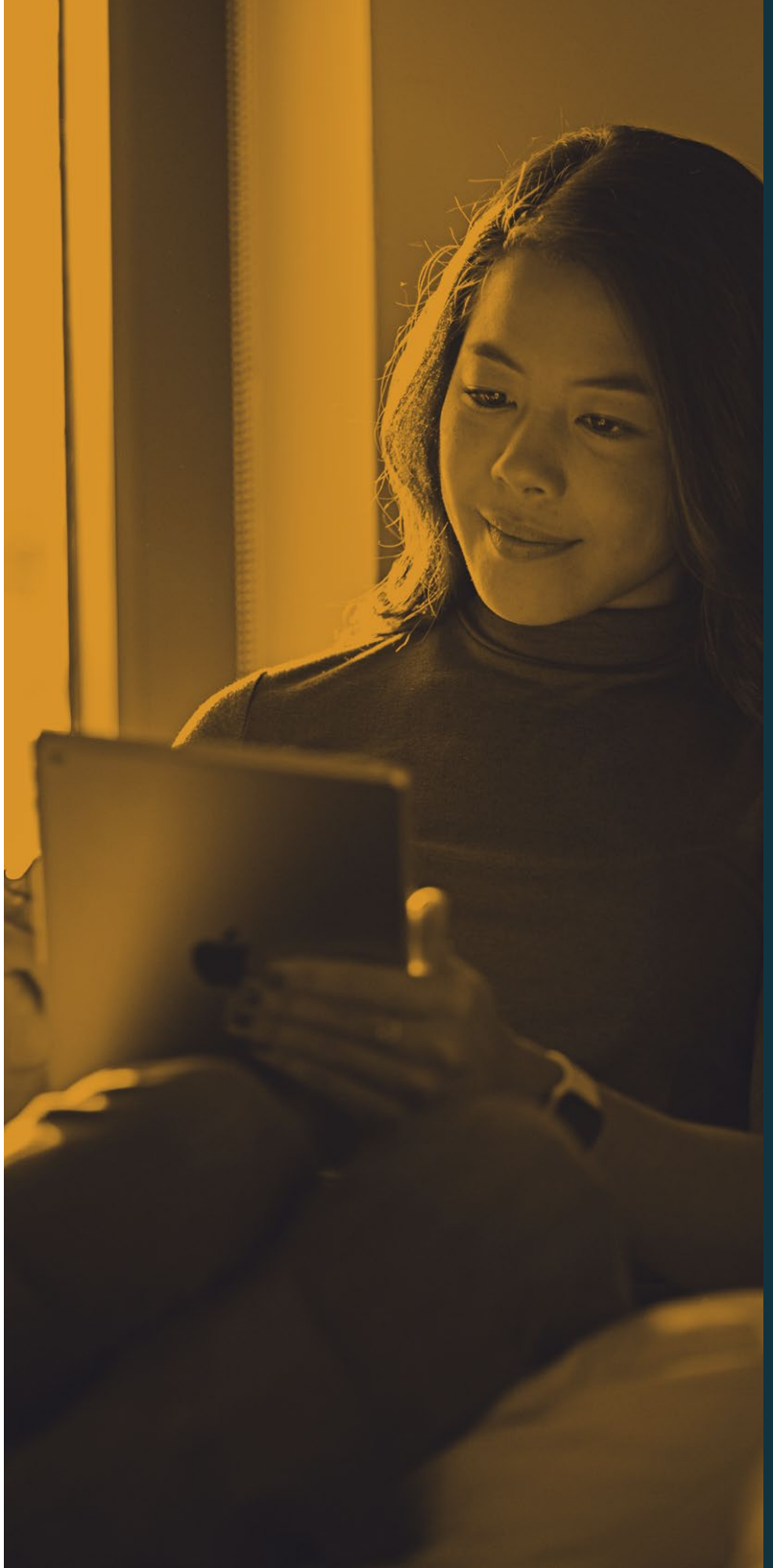
For those not sure as to what’s behind the spike in incidents, the answer is both simple and complex. The erosion of the network perimeter due to a shift to remote or hybrid work environments finds users utilizing mobile devices more to remain productive while working away from the office. That’s the simple part. The complex part is how organizations transform their infrastructure to keep devices protected and data secured.

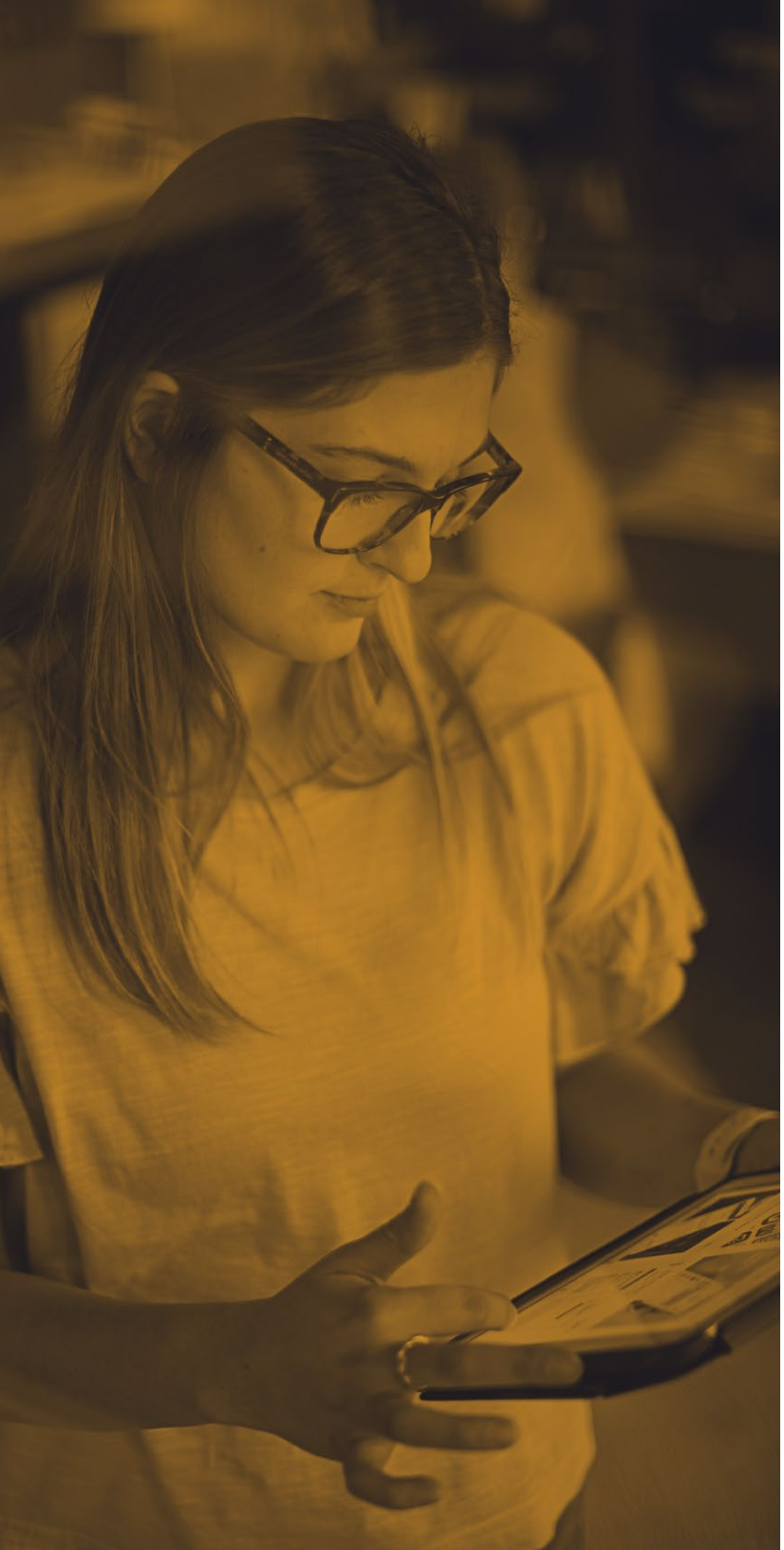
Minimizing the complexity involved, Jamf Threat Defense’s approach is a cloud-based one, mixing powerful, advanced security technologies with extreme flexibility and scalability. Including real-time monitoring, detection and reporting capabilities which allows IT and security teams to monitor the health of their entire fleet.

NETWORK PROTECTION

Among the multiple security threats modern enterprises are facing, phishing is only one of those types of threats, yet arguably it remains the greatest due to its targeting of the weakest link in the security chain: the user. The sad truth is that, even with well-meaning and trained users, the margin of error is still too high which is means success rates of compromise are high, therefore attackers will continue to leverage them in their attack chain.

By providing in-network protection, Jamf Threat Defense actively blocks zero-day threats like phishing websites in real time. In doing so, devices are protected from the effects of these campaigns before triggering the exploitative attack by preventing the device from accessing these malicious domains over all communication types: wired, Wi-Fi or cellular.





EXPANDING CAPABILITIES

Built with extending functionality in mind through integration with a vendor's API framework, Jamf Threat Defense boasts more Unified Endpoint Management (UEM) and Security Information and Event Management (SIEM) partnerships than other security solutions. What this means for IT and Security is that they can maximize the existing investment in security and device management appliances, apps and services to take advantage of threat insights, remediation workflows and automation.

One such excellent example of integration is when leveraging the Jamf risk API alongside the features of Jamf Threat Defense to enable unparalleled communication between both software platforms.
By doing so, data is shared between both systems in real time, allowing for customized reporting and remediation on the health of your organization's iOS endpoints.

ADAPTIVE ACCESS

One of the main reasons access-related threats are so effective is that if a device is compromised and there aren't any indicators that are visible to the user (aka- the device continues to operate seemingly normal), the user will still have access to a resource. The device will process the request and access will be granted, thereby compromising the resource as well.

Jamf Threat Defense simultaneously combats this and elevates your security posture by permitting only secure connections and trusted devices to access organizational resources. How does it do this, you ask? By continuously monitoring telemetry data and contextual inputs unique to each device for anomalies. Which, if determined that the endpoint is high-risk or compromised, will prevent access to the resource(s) through enforcement of customized policies.

After reading some of what Jamf Threat Defense can do to protect your enterprise and mobile device fleet, we'll dive a little deeper into the underpinnings of the software to give you a better look at how it weaves its magic to keep devices safeguarded from threats. Not features per se, but rather some of the built-in core defensive technologies that power the features mentioned above.

Jamf Threat Defense works tirelessly to thwart the myriad list of cybersecurity threats attacks that show no signs of slowing down and continue to plague the mobile security landscape.

ADVANCED MACHINE LEARNING

Let us introduce to you: MI:RIAM. Not a replacement for Siri or the newest member of the Wu-Tang Clan, but rather an advanced intelligence engine that works in real time to identify the broadest range of known and zero-day threats. By utilizing the largest set of threat data, MI:RIAM collects information from 425 million sensors worldwide as input for its algorithms, using advanced data science to provide real-time insight into the latest threat intelligence and active risks.

ALL DEVICES WELCOME

Only have iOS and iPadOS-based devices in your fleet? That's perfect. Jamf Threat Defense has exactly the type of security protections necessary to keep your Apple devices and user base protected against current and emerging threats.

Have other OS types in your mobile device fleet, as well? That's fine too! Jamf Threat Defense supports non-Apple device operating systems too and works just as hard to keep all your mobile devices hardened against threats, data safe and users unimpacted from being productive. Did we also mention that multiple ownership models, such as corporate-owned or the alphabet soup of BYOD, CYOD, COPE and COBO for the ultimate in flexibility without compromising on security.

“IT’S OUR SECRET… NEVER TEACH THE WU-TANG”

As a user, you want to know that you’re protected. As a member of IT, you want to know in what ways your users are protected. But when it comes to malicious actors, the less they know the better it is for maintaining your network’s security posture and ultimately keeping information safe. And there are several types of information you’ll want to keep safe at all costs to maintain its integrity, keep IT and security teams alerted to the latest health data of company endpoints and which security mitigation strategies are deployed to keep security at an all-time high.

USER PRIVACY

Personally-Identifiable Information (PII), including Personal Health Information (PHI) are among the grails of data types that threat actors seek to obtain. It’s a cyclical effect: the more they gather directly feeds how they will continue the attack while providing them a means to an end in their criminal endeavors. Thankfully, Jamf Threat Defense safeguards online privacy through encrypted communications, as well as protection against phishing attacks. This applies to not only the personal data of your users but also to sensitive information that may be be required to adhere to regulatory compliance. The advanced privacy features and policy controls follow the practice of zero trust conditional access and prevent access by risky users and/or devices.

REAL-TIME INSIGHTS

IT and Security teams can obtain detailed reports relating to endpoint health utilizing the default reporting features that are included or customize details by tuning them to fit the specific needs of your organization. Tailoring reporting features takes Jamf Threat Defense one step further, providing admins real-time data within the console, or exporting it to an SIEM partner through the built-in integration feature to visualize data on dashboards, or leveraging the API to integrate with a unified management solution, like pairing it with Jamf Pro, to stream data between the softwares, enabling automated device management and remediation of detected endpoint issues.

There's so much that you can do for your organization and your users, to keep data, devices and people protected. There was too much for us to even address in this e-book. So here's your next step:

Request Trial

Learn more by being hands on with a free trial of Jamf.
You can also work with your preferred Apple reseller to see what's possible with Jamf.

Either way, we're excited for you to get started.