Rethinking Endpoint Security for Modern Work

Endpoint security is generally accepted as keeping your device fleet safe from cybersecurity threats.

Though a substantial part of it, **there is more that goes into implementing and ensuring the endpoint security needs of your organization are met.** It's a set of capabilities that you need to protect your devices (and users) from a constantly evolving threat reality...and you'll need to choose the right tools to match the devices you've selected.

A lot more.

If you're new to the Apple ecosystem or perhaps this is first time tasked with managing endpoint security across the modern threat landscape for Mac or mobile devices, you need not worry, since Jamf is here to guide you through what modern management and endpoint security looks like, as well what that means for your remote or hybrid environment and the end-user, in light of old solutions and long held concepts that simply aren't right sized for these modern platforms.

In this Paper, we dive into:

What can go wrong?

For many organizations worldwide, managing Apple devices and ensuring endpoint security, while balancing the end-user experience, can be daunting task. Factor in that for every thousand devices deployed, two hundred of them are affected by insecure configurations and this may present great cause for concern.

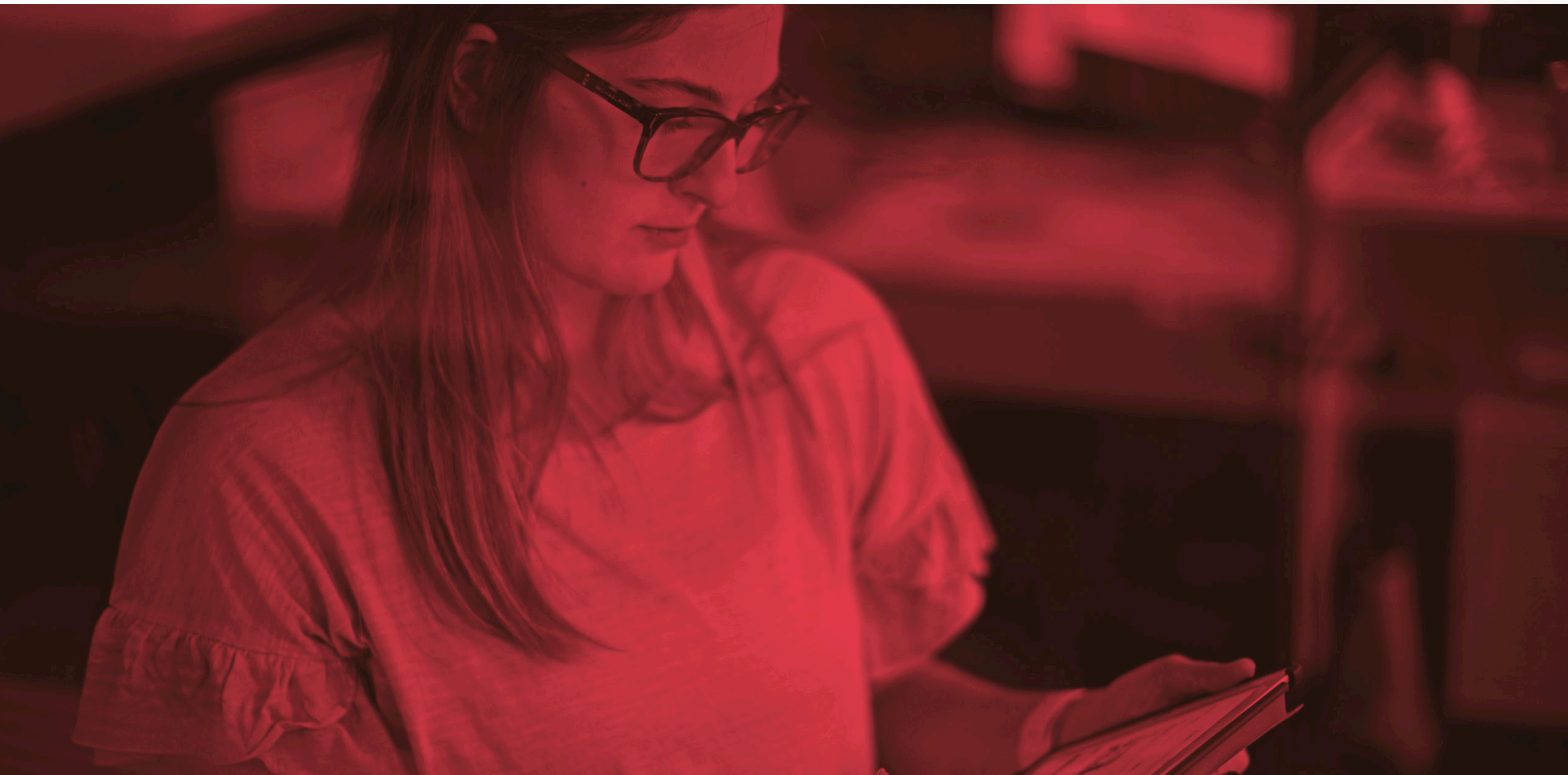
If it doesn’t, then that speaks to a bigger problem. It also paints a larger picture of what threats target organizations, such as data theft — either by permitting data exfiltrating over USB drives or over the network through credential loss by falling victim to phishing attacks or vulnerabilities in apps and the OS that are exploited because patches are not up to date.

Mitigating risk while keeping devices properly managed is tantamount to yin & yang. A balance between two seemingly unrelated aspects that come together — ensuring compliance by working in harmony — benefitting the whole.

Additionally, aligning security and management alongside compliance, like enforcing Acceptable Use Policies (AUP), prevents other forms of damage not purely technical in nature but all the same potentially disastrous. Examples of this are opening organizations to liability due to violating regulations that may govern your industry or damage to your company’s brand and/or reputation, such as that stemming from a publicized data breach.

39% of organizations allowed devices with known OS vulnerabilities to operate in a production environment with no restrictions to privileges or data access, **up from 28% in 2020**

— Jamf Security 360: Annual Trends Report



Maintain good device hygiene

So where do we start to effectively protect devices in a clear, concise and organized way? It all starts with a framework, that's how. One established upon three central pillars to provide layered protections in line with a defense in depth strategy that safeguards you from pitfalls such as:

Lack of insight into endpoint health: Unmanaged devices pose a significant threat to organizational resources and the security of company data and end users, permitting devices with questionable or unknown health status to access resources, potentially exposing data and user privacy.

Threats and vulnerabilities unchecked: Known and unknown malware threats, alongside network-based attacks, impact data security and integrity. Without the ability to communicate with endpoints regularly, devices may be out of date with patches and/or out of compliance without IT or Security teams becoming aware until its too late.

User-introduced risks and security concerns: Compromises to the security of your devices and/or the privacy of your users are often introduced through risky behaviors, such as downloading suspicious apps or violating acceptable user policies without enforcement.

Each of the three pillars below act as umbrellas that cover how security controls, best practices and guidelines essential to endpoint security should be used to keep your Apple fleet — both macOS and iOS-based devices — secured against modern threats, while data is protected and user privacy is preserved.

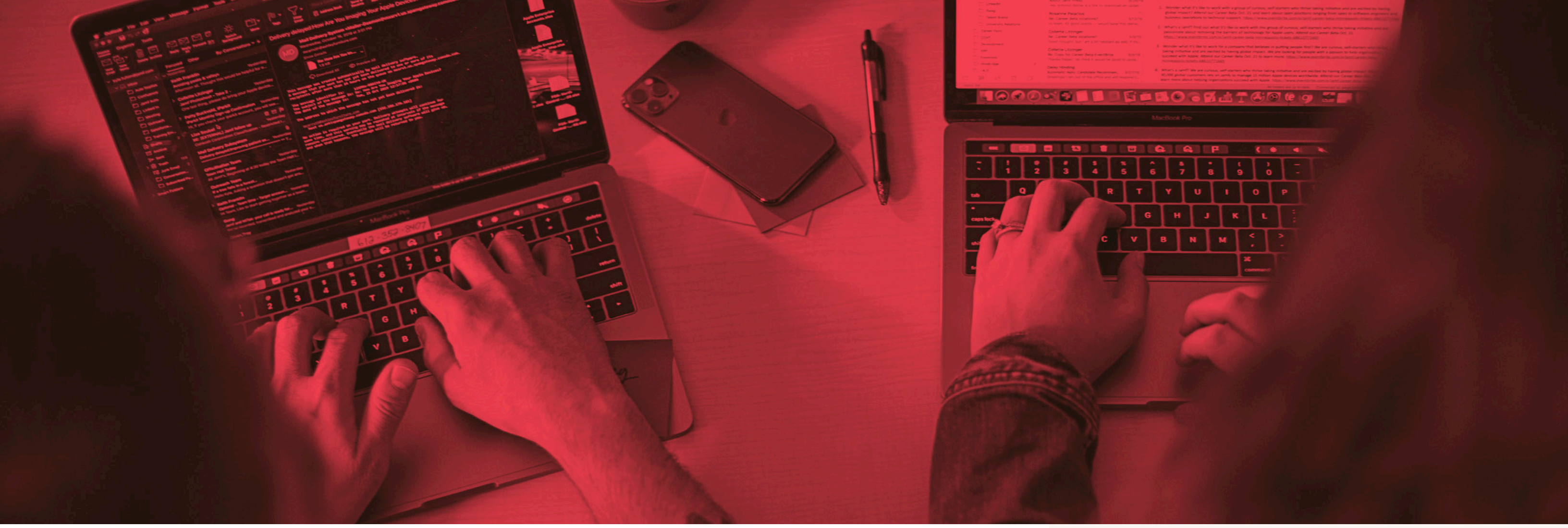
Furthermore, these pillars weave in the other half of the whole: management and how the integration between security and management form a comprehensive workflow to keep endpoints up-to-date, constantly monitored for compliance and ready to mitigate threats detected in an iterative cycle.

1 Establish secure baselines

Standardizing endpoint security helps organizations identify the needs that are unique to your device fleet. This informs management directly by prioritizing device hygiene while codifying security best practices into organizational policies helps to align needs with the hardening standards that will address risk quickly and in a manner that is easy to understand.

Vetting applications prior to deployment and keeping the OS and apps up-to-date not only ensure that applications and supported operating systems adhere to best security practices, but ensure that both IT and Security teams are supporting software that works with your organizational needs — not against them — keeping vulnerabilities to a minimum while standardizing organizational support.

A critical aspect to this is managing user privilege controls, such as permissions. By limiting access rights using the principle of least privilege alongside managing device settings, users are limited only to accessing data and performing tasks that are required for them to remain productive — all other rights are secured to prevent abuse.



2 Defend the device from modern threats

Integrating endpoint security with management — not keeping the two isolated — is table stakes to keeping both Apple computers and mobile devices, and users and data, safely guarded against modern device- and network-based threats. Threat intelligence data shared between management and security — both aligned to Apple's Endpoint Security Framework (ESF) — centralizes management policies, automatically triggering workflows to remediate issues while alerting IT and Security teams.

By consistently monitoring for CVE threats, signature-based analytics categorize and prevent known threats from impacting your endpoints. Similarly, behavioral analytics and advanced ML identify and mitigate unknown threats or zero-day attacks before they have a chance to compromise your endpoints. Through constant monitoring and reporting of device health status, security solutions keep IT and Security teams updated through granular reporting. Furthermore, real-time alerting functions loop in support teams when endpoints require triage or remediation.

Lastly, centralizing threat intelligence sharing between management and security delivers organizations compliance-relevant data. This level of information permits support teams to mitigate risks when identified to bring endpoints back into compliance before threats can lead to larger security issues, such as lateral movement or data theft that may result in damage to the company's reputation or exposure to legal liability.

7% of compromised devices accessed cloud storage services (such as OneDrive, Google Drive and DropBox) and 25% accessed email services (such as Gmail and Outlook).

Source: Jamf's Security 360: Annual Trends Report

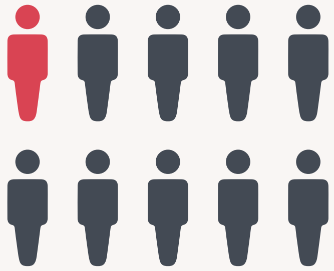
3 Managing user-initiated risk

Users present the largest threat to endpoint security by far. Whether actions are performed maliciously or unintentionally, the result often leads to the same conclusion: risky behaviors pose a genuine threat to the security of your Apple fleet and critical or sensitive organizational data.

Aligning security and management addresses user behaviors that could potentially introduce risk by relying on behavioral analytics to determine if risky behaviors, such as malicious downloads or accessing websites used in phishing attacks, regardless what device ownership model is used.

As such, security processes must be able to secure endpoints while management enforces compliance with organization policies, like an Acceptable Use Policy.

Speaking of protecting privacy, modern computing environments often support a mix of ownership models, including BYOD. While offering the same level of privacy protections to personal devices as it does company owned endpoints, management and security must be flexible to not overreach and instead focus on preserving end-user privacy without compromising security — and vice-versa.



1 in 10

people click on phishing links while on their mobile devices

Source: Wandera, a Jamf Company

The number of mobile users falling for phishing attacks has increased by 160% YoY

Source: Wandera, a Jamf Company

Why are security tools needed on top of Apple native features?

Apple is regarded as developing some of the most secure, out-of-the-box devices. Leaning into its Unix underpinnings and combining with Apple's historic doubling down on security and privacy, Mac comes packed with native protection software and technologies that limit its exposure to security threats, including:

XProtect: Antivirus software providing signature-based detection of malware

Malware Removal Tool (MRT): Automated removal of detected malware

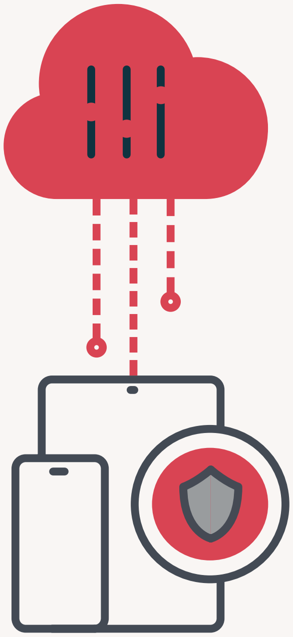
Notarization: App scanning service that provides a digital ticket to software found to be free from malware

Gatekeeper: Works with notarization to ensure only trusted software runs on your Mac

Sandbox (Containerization): Contains damage to your Mac in the event that user data becomes compromised

App Store: Secure method of distributing trusted apps, managed by Apple

Asked another way, do IT and Security teams have visibility into the latest threats targeting the Mac in your organization? Without purpose-built security and management solutions, the answer is a resounding **no**. The quantity and types of threats targeting Apple require layered defense strategies, flexible support for varied ownership models and a centralized management capability at a minimum to meet the varied and increasing demands of the modern threat landscape.

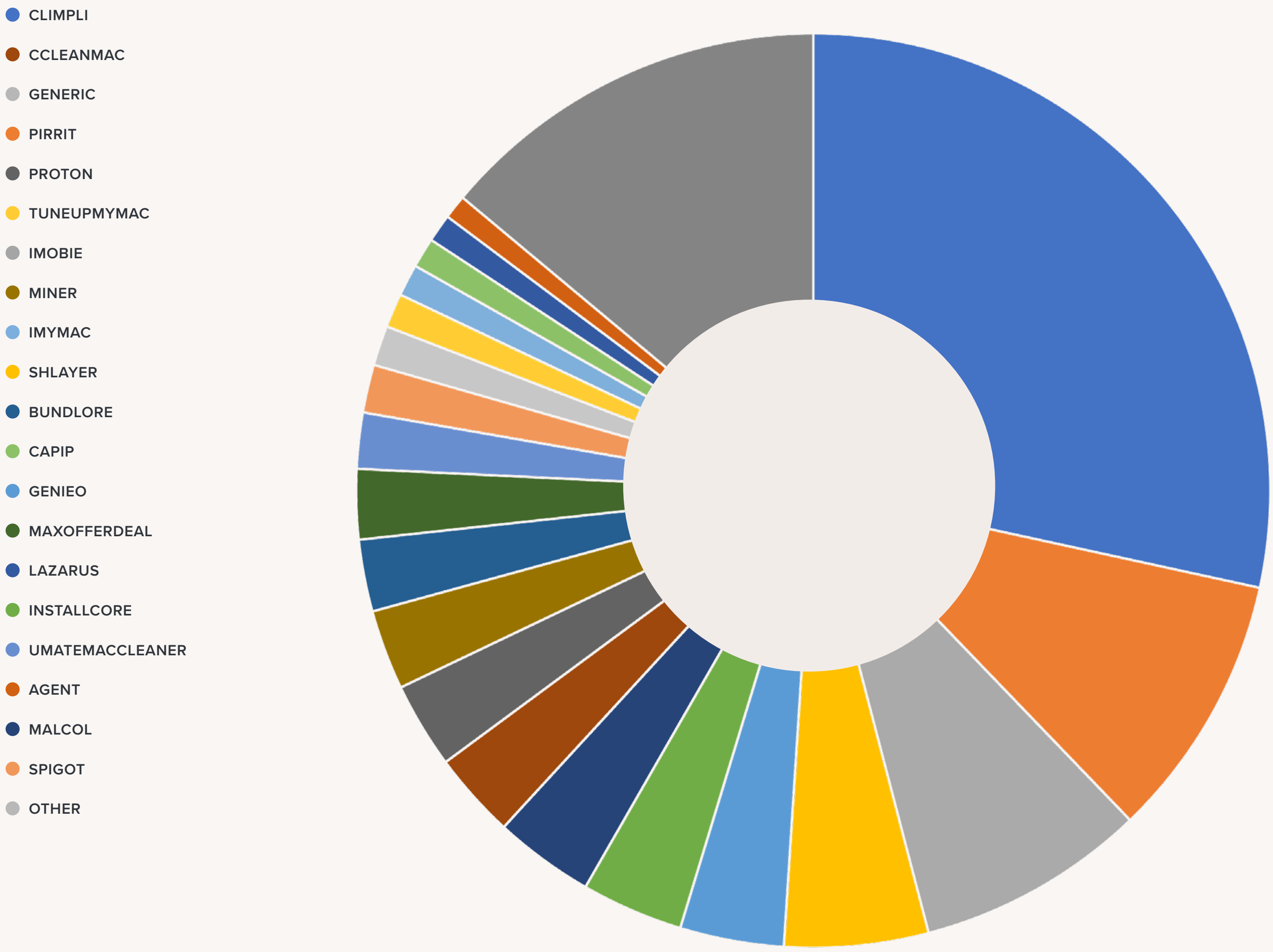


Fun fact:

In 2021, **6% of organizations** experienced a malware installation on a remote device, **up from 3% in 2020.**

Source: Jamf's Security 360: Annual Trends Report

The share of Mac malware families detected in 2021



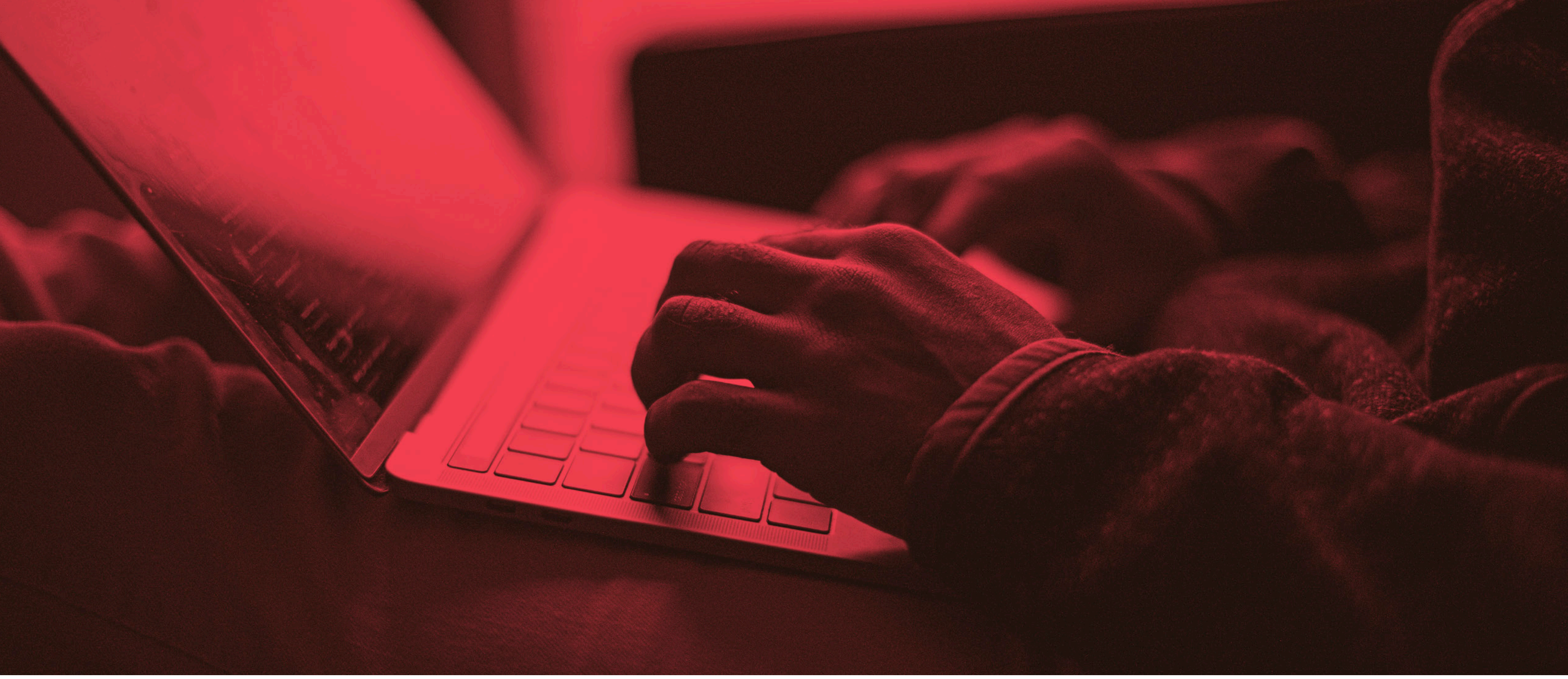
Source: Jamf Threat Labs

Layers of defense

Thus far, we've discussed the potential risk to organizational data, plus the three pillars that make up the basis for a modern, layered defense strategy with management and security as equal anchors to your endpoint security plan.

We continue down this path incorporating additional concepts, components, technologies and practices to more fully flesh out an endpoint security plan that meets your organization's unique needs, working to address security comprehensively across your entire fleet by mixing in best of breed solutions, designed specifically for Apple-centric endpoints, while supporting user choice models.

The key here is to make integration a natural extension of security and management, working with and expanding existing infosec workflows while elevating the user experience — not damaging it.



User choice

COPE/BYOD/CYOD are ownership levels in modern computing but the security and manageability of endpoints must remain the same if data is to be secured and threats prevented against. Finding a solution that is powerful, yet flexible enough to address risk appetite while permitting users to work comfortably on any device from anywhere should be the goal.

Choose best of breed

Don't settle for a solution that offers minimal support for the Apple ecosystem simply because it also manages Windows devices. The perceived benefit to eliminating administrative overhead quickly loses its value when compared to best of breed solutions, tailored specifically to Apple devices, supporting all features from the first day. You should decide when and how to manage your endpoints — not have it dictated by your security or management software.

Integrate with existing infosec workflows

There's no need to reinvent the wheel, especially if you have mature workflows that address your organization's needs and those of your users. This is one place where integration pays dividends for IT and Security teams by marrying their existing workflows with best of breed solutions to augment foundational security and management — not tear it down due to incompatibility or lack of developer support.

Elevate user experience to a key solution

Let's face it, users are often relegated to being told what they can and cannot do. In the modern computing landscape, with remote work and BYOD programs in place, end-users need to be considered as part of the solution — not a problem that needs protection from itself.

Endpoint security is a foundational capability

Remember yin & yang — endpoint security goes beyond antivirus installed on your Mac or VPN configured on your iOS-based device. The modern threat landscape sees security (yin) and management (yang) working seamlessly together as one holistic, Apple-focused solution that serves as the foundation to the myriad technologies, practices and policies that make up your defense in depth plan while enforcing endpoint compliance.

Misconceptions of all-in-one solutions

A centralized stack refers to the ability for both solutions to work together as one cohesive unit (again, think yin & yang) offering holistic benefits from the inclusion of both halves. It should not be misconstrued as a single solution to perform the heavy lifting in place of both, usually under the guise of a “single pane of glass”, as these one-size-fits-all solutions often manage multiple OSs but at the cost of offering full support for any solution, resulting in a lack of efficiency and efficacy when addressing Apple-centric endpoint security.

Integration between solutions - win-win

Unifying management and security operating as one impenetrable force, begins by sharing the data that both teams rely on in order to carry out their respective functions. Moreover, integrating all necessary tooling and workflows to form a single solution helps support teams refocus their efforts to empower users, instead of scrambling to find and resolve issues. From gathering data to assessing device statues, generating reports and managing real-time alerts – all can be managed simply, while implementing workflows to triage and remediate detected and/or suspected issues before threats can lead to something far worse, like a data breach.

Security vs performance? Why not both?!

Security is often viewed through the prism of compromise. In order to gain more protection, stakeholders must give up certain liberties. But new technologies, such as Zero Trust Network Access (ZTNA) with its context-aware policies, flips this notion on its head by not trusting endpoints nor their connections. Instead, ZTNA focuses on keeping data secured against unauthorized access and threats to data integrity, providing both security and performance without compromising either or the user experience.

The number of organizations with a potentially unwanted application installed within their fleet more than **doubled from 5% to 11%.**

36% of organizations encountered **malicious network traffic** indicators on a **remote device in 2021”**, which begs the question: **Are your IT and Security teams able to react quickly to indicators of compromise?**

Did you know:

34% of compromised devices accessed conferencing services **(such as Zoom, Skype and Microsoft Teams)** in 2021. That number increased to **64%.**

Source: Jamf's Security 360:
Annual Trends Report

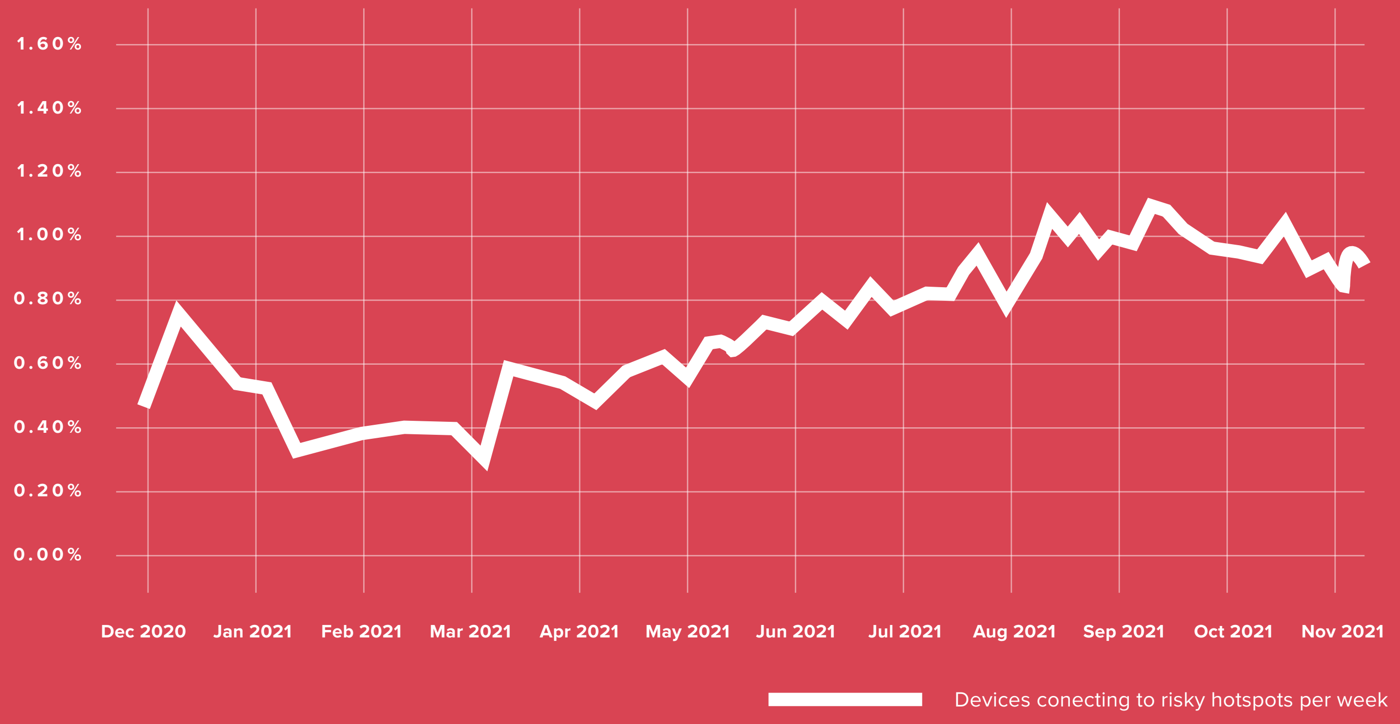
Empowering your users

The user matters. And technology should flow as an extension of the user, empowering them — not restricting or blocking them from being productive in any manner and fitting hand in glove within the contexts of how and where they feel most comfortable. After all, their comfort level adds to them being a happy user, and a happy user will always be more productive than an unhappy one. This goes doubly when considering modern work environments, based on employee choice programs and BYOD initiatives. Combining this with the shift in moving the infrastructure to the cloud, all in support of the remote and hybrid work environment.

According to Jamf Threat Labs data, “The number of mobile users falling for phishing attacks has increased by 160% year over year.”

Source: Jamf's Security 360:
Annual Trends Report

Devices conecting to risky hotspots per week



Source: Jamf's Security 360:
Annual Trends Report

Key takeaways:

- ☑ Assess your endpoints to determine what modern protections are necessary to meet security requirements
- ☑ Adopt a framework that is purpose-built and tailored to protect Apple devices and serves as the foundation of your endpoint security strategy
- ☑ Prevent malware, identify vulnerabilities and monitor suspicious and risky behaviors while mitigating risk and deploying patches through policy-based workflows to keep devices compliant
- ☑ Establish and maintain secure baselines that set the standard for device hygiene
- ☑ Extend Apple native protections so security teams have visibility into threats impacting the business
- ☑ Integrate security and management to seamlessly deploy solutions and rapidly mitigate threats when they are discovered
- ☑ Choose best of breed solutions that fully support the Apple ecosystem from first day of release and align with Apple-designed frameworks – so users can enjoy a great experience and IT can upgrade on their schedule
- ☑ Preserve the Apple experience while augmenting security and maintaining performance
- ☑ Support all device ownership models to maximize securing users, devices and data while preserving the end-user's privacy
- ☑ Empower your users to be productive with the device they feel most comfortable with and where they feel most comfortable working from

Learn how Jamf offers a complete purpose-built solution to protect users from malicious intent — all while maintaining minimal impact to the end-user experience. Or, request a trial and see how you can protect your users.

Request Trial