Security 360:
Annual Trends Report

Jamf's annual data-driven security report looks at threats and their impact on organizations globally, plus offers practical advice on how to configure business tools to ensure fast and safe connectivity for all users in 2022.

Key findings

The percentage of organizations that experienced a malware installation on a remote device doubled from **3% in 2020 to 6% in 2021**.

In 2021, 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**.

7% of work devices continued to access cloud storage services after being compromised **in 2021**.

Over the course of **2021**, the number of devices connecting to risky hotspots per week **doubled from 0.5% to 1%**.

1 in 10 users fall victim to phishing attacks on remote devices.

Source: Jamf Threat Labs

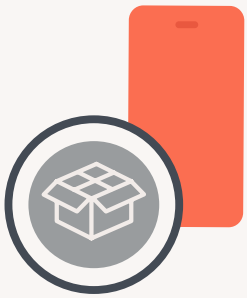
Introduction

At the dawn of the global pandemic, organizations were faced with the grueling task of ensuring business continuity while simultaneously transitioning to a hybrid or fully remote work environment at a moment's notice. Two years later, the work landscape has largely adopted remote access technologies and cloud-based software to allow employees to work from virtually anywhere and access company data at any time, on any device. But how has this impacted the security posture of businesses globally?

Each year, we analyze the threats impacting devices used in the modern workplace. As the workforce has become more distributed, so too has our perspective on the threat landscape.

This year's report will look at five key security trends impacting real organizations with users that are connecting remotely to a multitude of apps hosted in private and public data centers via a variety of portable devices and platforms.

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



Less than 1% of organizations had a jailbroken or rooted device in **2021.**

Trend 1 — Adapting security strategy for the distributed workforce

With the shift to a more permanent remote workforce, there has also been a shift in the way security is delivered. Rather than traditional on-premises solutions that focus on protecting the assets within the office and the corporate network, businesses have worked to decentralize and distribute their security services to the endpoints that produce and consume data and to the cloud applications that store and use data. This results in more capable and self-sufficient endpoint security, and more resilient and robust application security.

Remote access technologies that connect the distributed, remote endpoints and the distributed, cloud-hosted applications can be adopted to intelligently allow and deny access per device and per application. Part of that process is deciding what risk indicators should trigger a decision to deny access to corporate applications. Risk and compromise indicators are subjective. If an organization has a high tolerance for risk they might require device compromise indicators to be present before denying a connection to a corporate application. While compromise indicators are subjective, Jamf Threat Labs' standard device compromise indicators include: (1) malware installation and (2) a Jailbroken or rooted device. According to Jamf Threat Labs data, compromised devices are quite uncommon but are still impacting real users and organizations.

These two datapoints above suggest that users are tampering with their devices a lot less than they used to; and bad actors are increasing their attacks on company devices.

Source: Jamf Threat Labs

Organizations with a lower tolerance for risk might want to deny access when any vulnerability or compromise indicator is present. While vulnerability indicators are also subjective, Jamf Threat Labs' standard vulnerable device indicators include: (1) vulnerable operating system, (2) unwanted application present, (3) third-party app store present, and (4) other device compliance violations and misconfigurations.

These risk indicators were also present within our data in 2021:

In 2021, 39% of organizations were regularly utilizing an operating system with a known security vulnerability, up from **28% in 2020.**

Over the course of 2021, the number of organizations with a potentially unwanted application installed within their fleet more than **doubled from 5% to 11%.**

This refers to any app that isn't proven malicious, but risks introducing threats into the environment by allowing the user to circumvent policy or introduces inappropriate content (e.g., via malicious ad networks).

Over the course of 2021, the number of devices that had a third-party app store installed **increased from 1% to 4%.**

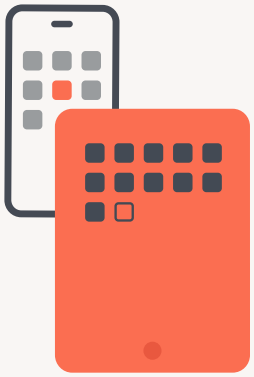
In 2021, 5% of devices, or 20% of organizations, were impacted by risky device configurations.




While the percentage of devices that are compromised or vulnerable is low, it's alarming to look at how many of these devices are accessing sensitive assets.

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) **in 2021.** Those numbers increased to **9% and 48%** respectively when including the vulnerable device indicators above.

9% of compromised devices accessed a CRM (such as Salesforce and Microsoft Dynamics) and **34%** accessed conferencing services (such as Zoom, Skype and Microsoft Teams) in **2021.** Those numbers increased to **15% and 64%** respectively when including the vulnerable device indicators above.



But there's no use defining a remote work security policy based on the above data if you don't have the tools needed to assess risk and enforce access decisions in real-time. Legacy remote access technology such as VPN certainly won't cut it.

Global adoption of VPN technology used to encrypt traffic over unsecured communication lines grew in 2020, though the shift to cloud-based applications saw this growth scale downward in 2021, with 43% of users admitting that "I know what it is, but I do not use one", as part of a survey conducted by security.org.

Not bad for a security technology that was developed over twenty-five years ago. And while using VPN is better than no protection at all, the limitations of VPN combined with the fact that computing has changed a lot in the last couple of years has seen the birth of more modern approaches to remote access, such as Zero Trust Network Access, or ZTNA. A set of security technologies that offer dynamic protection to meet the needs of new networking technologies such as Wi-Fi and cellular, breaking the many assumptions VPN was built on. The technology gets its name by never inherently trusting a user or device, unlike VPN. Instead, ZTNA allows connections to apps and services only after verifying that the device and user are allowed access to the requested services and meet the minimum "health" requirements to do so securely.

ZTNA is designed with modern networks and workflows in mind by integrating with cloud-based identity providers (IdP) to leverage permissions based on explicit user access rights. Privacy-aware ZTNA solutions mitigate risk and safeguard data, while being flexible enough to ensure that personal apps and data remain private, further maintaining user privacy. Furthermore, authorized users only have access to connect to the apps they are allowed to access; this prevents attackers who compromise that one user from accessing all of the applications in the catalog.

Trend 2 – Threat actors have pivoted tools and campaigns to take advantage of the devices users are choosing to work on

As organizations adopt new technologies to secure their communications and maintain business continuity in the face of ever-evolving processes, threat actors have been busy upgrading attack methods and targets to improve their efficacy.

The attack categories remain the same, but, specifically, how they are executed by attackers has been augmented to account for the fact that users are now outside the confines of the traditional office and working on more consumer-friendly devices, such as smartphones, tablets and laptops, and increasingly, they are choosing Apple devices. According to a recent survey almost 90% of employees would take a pay cut to use the platform they prefer, while 62% of them will choose Apple when they can.

While confirmed malware infections remain low, malicious network traffic is more prevalent. Malicious network traffic refers to network-based Indicators of Compromise (IoCs) that can be observed in the communication patterns between the device and Internet servers; these signals can include data exfiltration or connections to command and control servers or sites known to host malware.

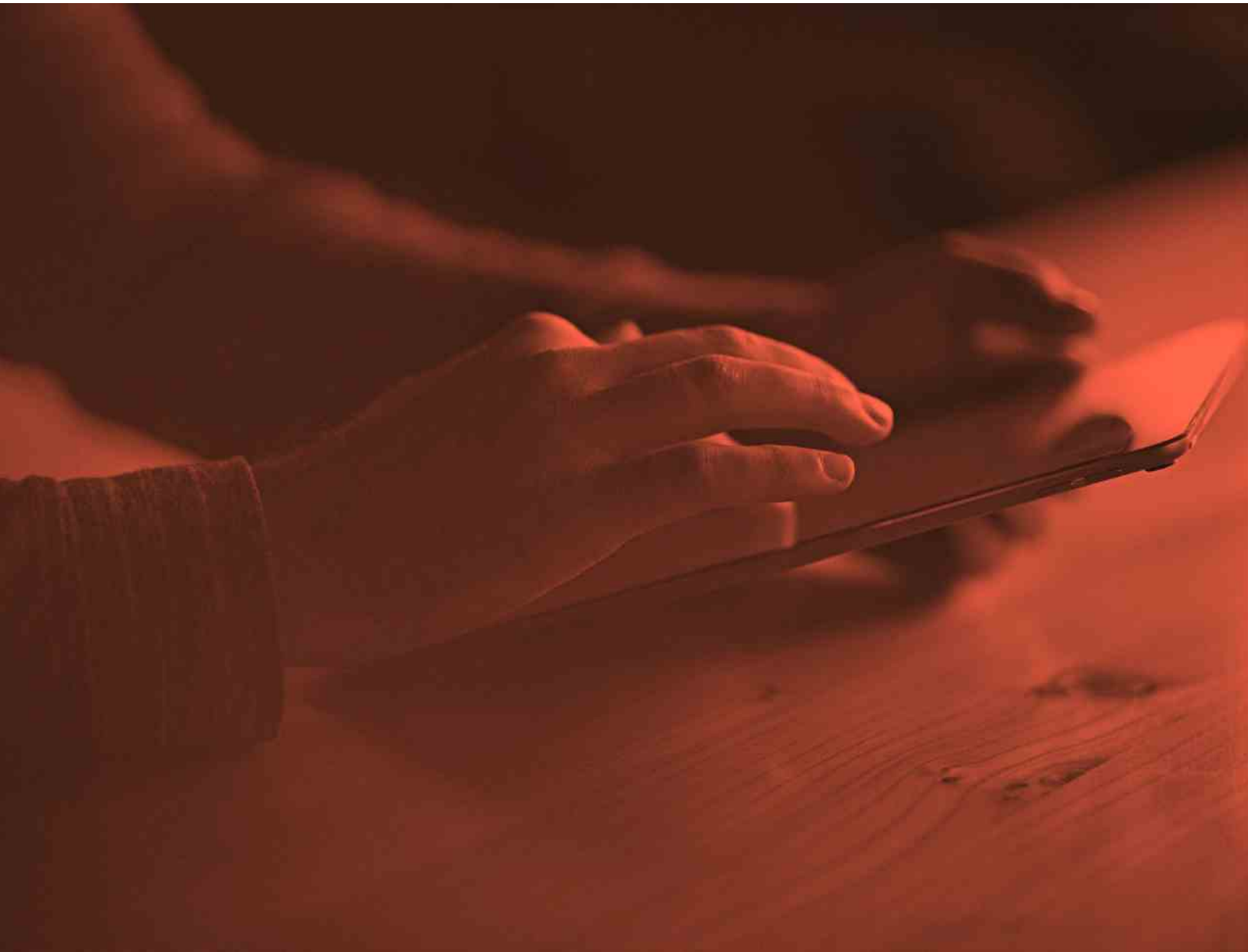
36% of organizations encountered malicious network traffic indicators on a remote device in **2021.**

Source: Jamf Threat Labs

Malicious network traffic is typically only observed in production environments, and cannot be identified by simply assessing static code, which is why monitoring for this indicator is so important beyond the official app store security checks.

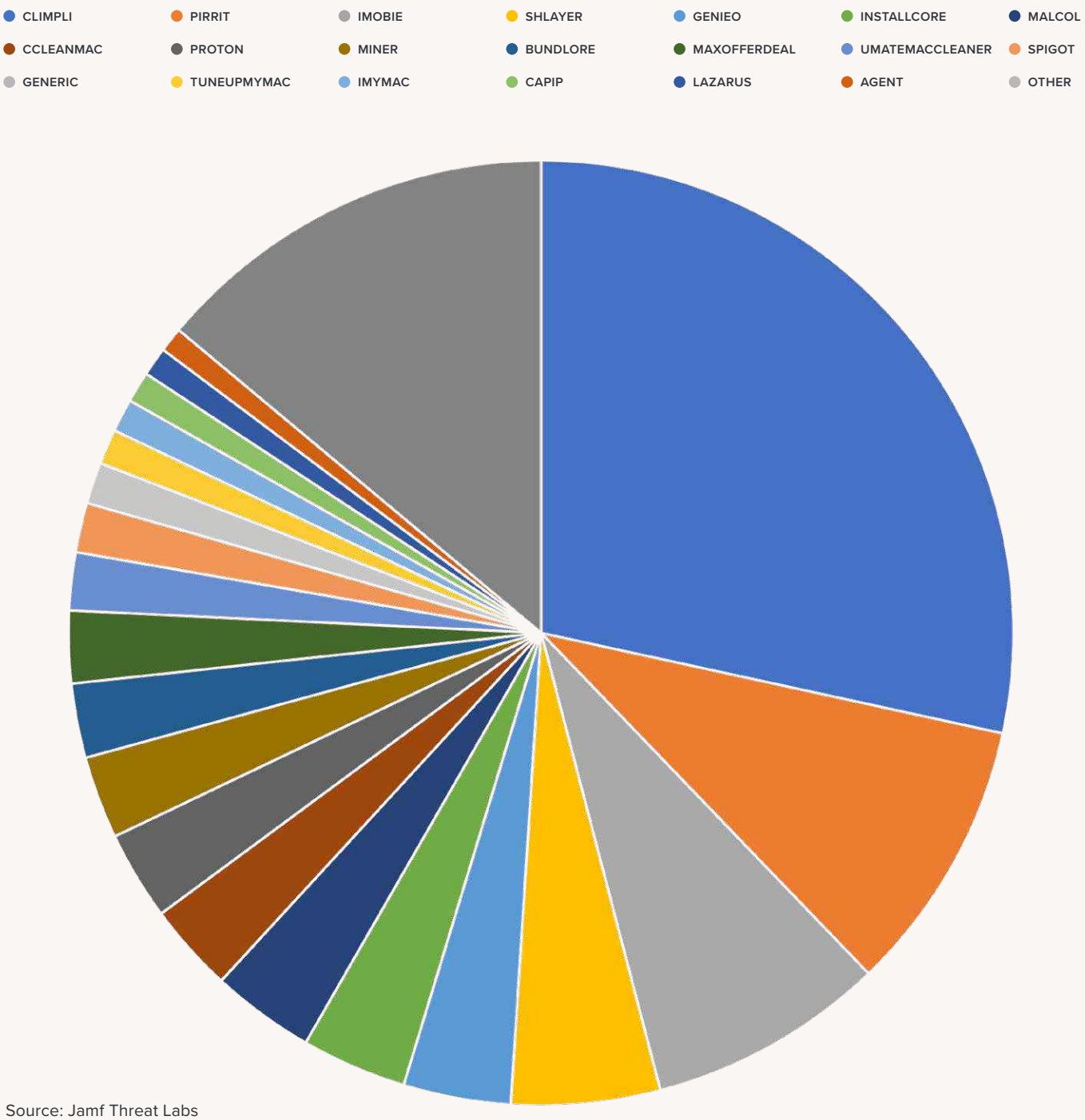
Mac malware is becoming a problem. In 2021, Jamf Threat Labs announced the discovery of a new variant of **Shlayer malware**, which allowed an attacker to bypass Gatekeeper, Notarization and File Quarantine security technologies in macOS. The exploit allows unapproved software to run on Mac and is distributed via compromised websites or poisoned search engine results.

Also in 2021, Jamf Threat Labs discovered **a zero-day TCC bypass in XCSSET malware** that allowed an attacker to bypass Apple's TCC protections which safeguard user privacy. By leveraging an installed application with the proper permissions set, the attacker can piggyback off that donor app when creating a malicious app to execute on victim devices, without prompting for user approval to access or use hardware features, such as the camera or microphone, for example.



Many people don't realize there is malware affecting modern Mac devices. **The below chart represents the share of Mac malware families attempting to compromise devices protected by Jamf in 2021.** The top 5 were Climpli, Pirrit, Imobie, Shlayer and Genieo.

The share of Mac malware families detected in 2021



Source: Jamf Threat Labs

The growth in remote work has given rise to security threats targeting not just devices and applications, but the users themselves more aggressively, with threat actors pivoting phishing campaigns towards targeting modern cloud applications used for work, such as Office 365 and Google Workplace (formerly G Suite) apps. As businesses strive to move their corporate assets to the cloud, this is a major concern. One slip up by an employee who receives a clever phishing attack (e.g., asking them to confirm their Box login credentials) can give a bad actor access to corporate assets stored on these types of popular cloud applications.

According to Jamf's study: **Phishing Trends Report 2021**, which was published in Q4, 2021, the top three brands used in phishing attacks that were successfully used to trick users into parting with sensitive data in 2021 are Apple, PayPal and Amazon, which account for 43%, 27% and 9% of those attacks respectively. These attacks reached devices across multiple operating systems not just Apple devices despite the Apple brand being the most used brand in attacks. It's worth noting that these brands haven't done anything wrong, they are simply being used by attackers because of the recognizable name.

Additional considerations affecting the mobile space is a significant rise in smishing, or SMS-based phishing attacks, that find users receiving maliciously crafted SMS/text messages from spoofed origins in a concerted effort to compromise accounts through impersonation. Attack focus ranges from email to banking, social media and even attempting to fool users into divulging legitimate two-factor authentication codes received from actual services to further extend their reach into realms secured with multifactor authentication technology. Users are likely more susceptible to phishing on mobile due to smaller screen sizes, hidden URL bars, inherent trust in the device and apps, as well as the rushed and distracted nature of mobile use. According to Jamf Threat Labs' data, 1 in 10 users fall victim to phishing attacks on mobile.

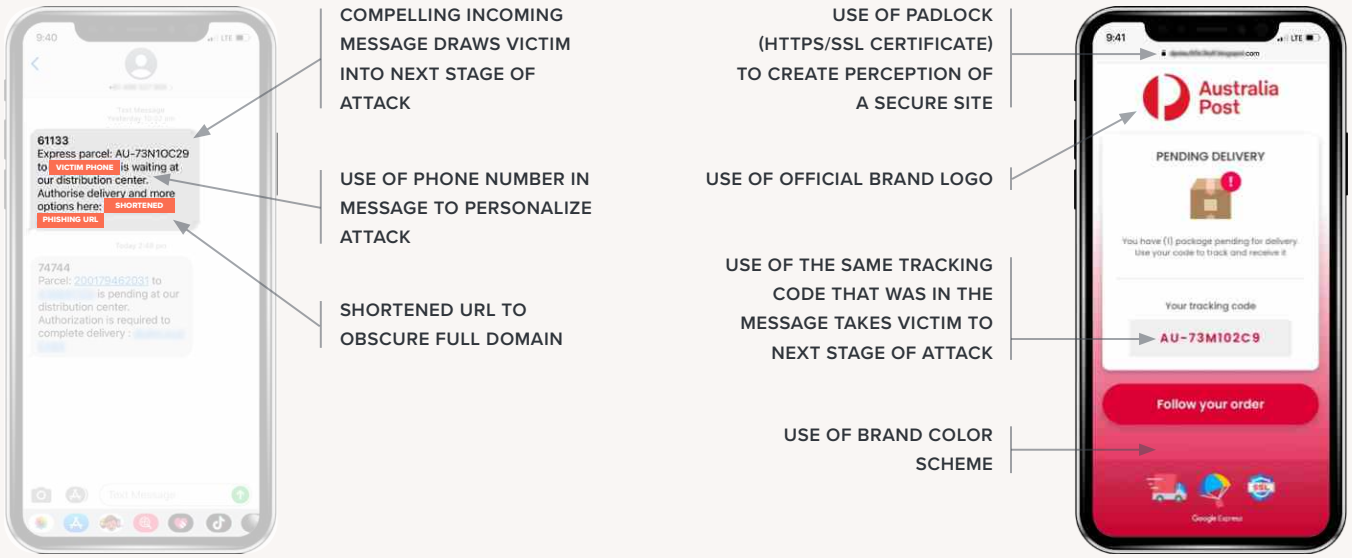
Phishing Trends Report 2021

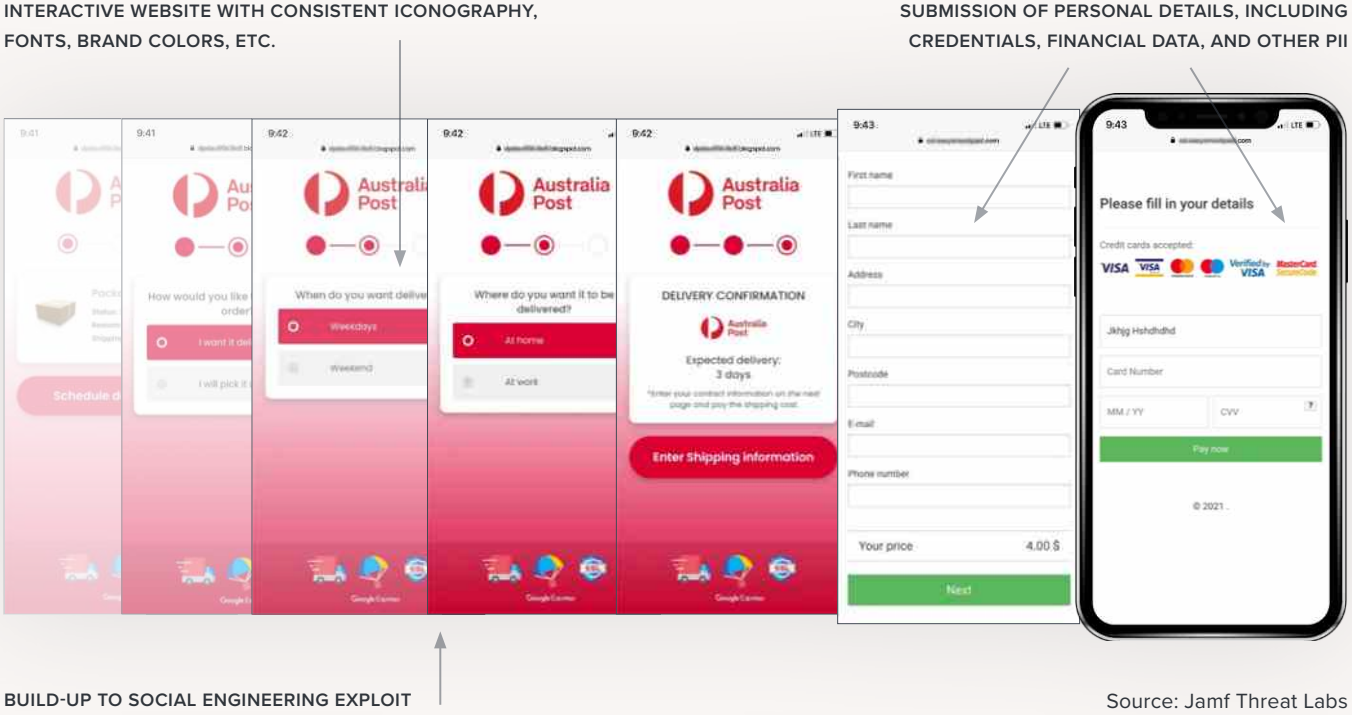
Top 10 brands used in phishing campaigns in 2021

1. Apple
2. PayPal
3. Amazon
4. Chase
5. Facebook
6. Google
7. Twitter
8. Netflix
9. Microsoft
10. Wells Fargo

Source: Jamf's Phishing Trends Report 2021

Jamf Threat Labs investigated a mobile phishing campaign when multiple suspicious text messages were identified using similar tactics and seeking the same sensitive PII from users. The messages were themed around package delivery, using the well-known Australia Post brand (Australia Post is the equivalent of the USPS in the US or Royal Mail in the UK, so the pool of potential victims is anyone that lives in Australia and receives mail). An opportunistic attack given how much people were relying on home delivery during Australia's strict and repeated COVID-19 lockdowns. Like the other major brands being used in phishing attacks, Australia Post hasn't done anything wrong, the brand is simply being used by attackers because of the recognizable name.





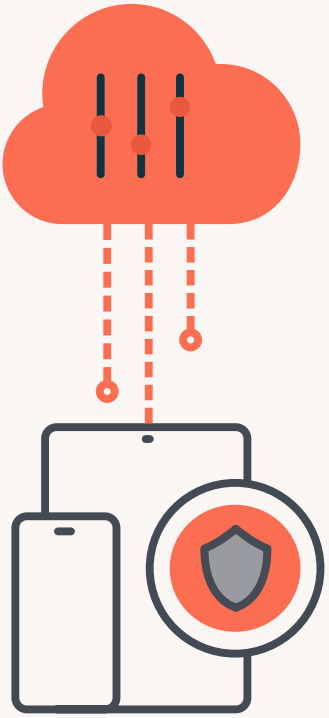
Source: Jamf Threat Labs

Trend 3 — Balancing security needs while maintaining user privacy is paramount

It is estimated that in 2022, the number of users with access to mobile technology will be 7.26 billion – **approximately 89.76% of the world's population**, according to forecast figures by Ericsson and the Radicati Group. With access to multiple network communications for ultra-fast connectivity, multi-core hardware, and extended battery life, it's no wonder why more and more users are relying on mobile devices to perform work tasks in addition to personal ones.

Companies are also banking on this trend by supporting many flavors of device ownership, including BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), COPE (Corporate owned, Personally Enabled) and COBO (Corporate Owned, Business Only), to meet the needs of the organization and its user base, whether it be shifting cost, enabling productivity, or providing choice to employees.

However, while IT and Security teams are concerned with security-related processes and workflows, end-users are concerned with their privacy and autonomy. More to the point, how much of their online use is visible to employers, and how will the use of their devices be impacted by security and management tools.



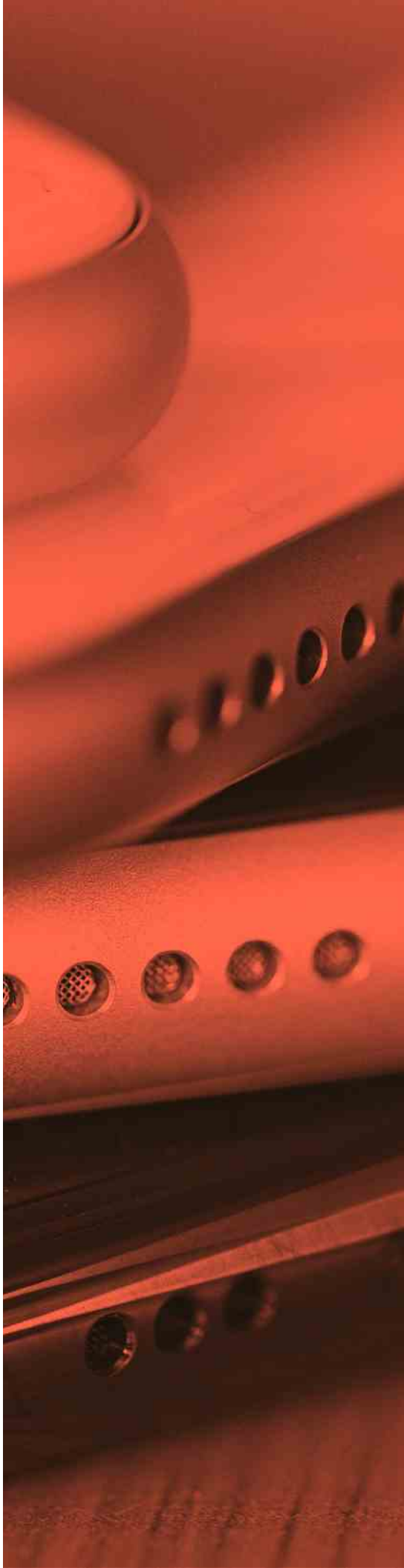
While security is of the utmost importance, the importance of privacy cannot be understated – especially when users are provided company devices (or submitting their own personally-owned devices). The question that begs: Does the right to privacy eclipse security concerns or do security process requirements upstage privacy concerns?

The answer is not as clear, depending greatly on the environment and other mitigating factors, such as regulatory requirements and who retains ultimate ownership of the hardware itself. With that said, Apple is leading the charge by providing frameworks for the apps that run on its devices to protect the right to user privacy. Apple recently introduced new privacy controls in macOS Mojave that require users to manually enable access to cameras and microphones, location information and network connections, etc., so now apps and services that utilize these functions will install with access disabled by default to protect end-users from unauthorized monitoring.

Intrusive device management and security solutions aren't the only privacy issues facing users. App developers can also encroach on user privacy, particularly when apps are free, they are likely to be monetizing user data instead.

According to Jamf's study: **An Analysis of iOS App Permissions**, which was published in Q2 2021, the most common permission requested is photo library access with 66% of the iOS apps included in our study requesting access, followed by camera (60%), location (58%) and microphone (34%). And there were quite a few suspect app categories requesting access they don't need. For example, it makes sense that the majority (62%) of navigation apps request access to your location, but why do almost half of them (48%) also request access to your camera? Same story for the 83% of shopping apps requesting access to your camera. It makes sense for scanning QR codes, but why do so many (87%) also request access to your photo library? It pays to think about what an app actually needs to function before hitting accept.

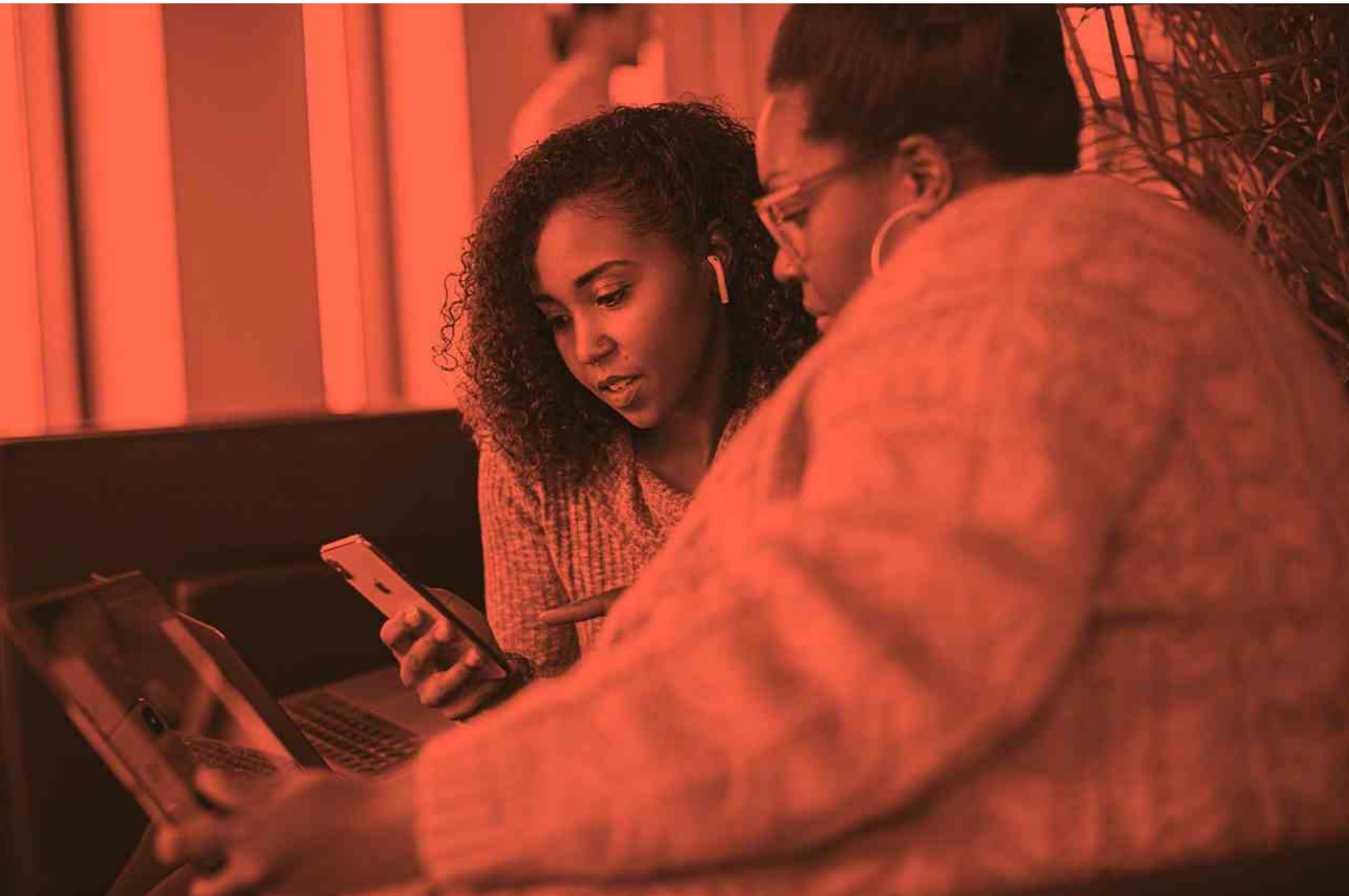
An Analysis of iOS App Permissions

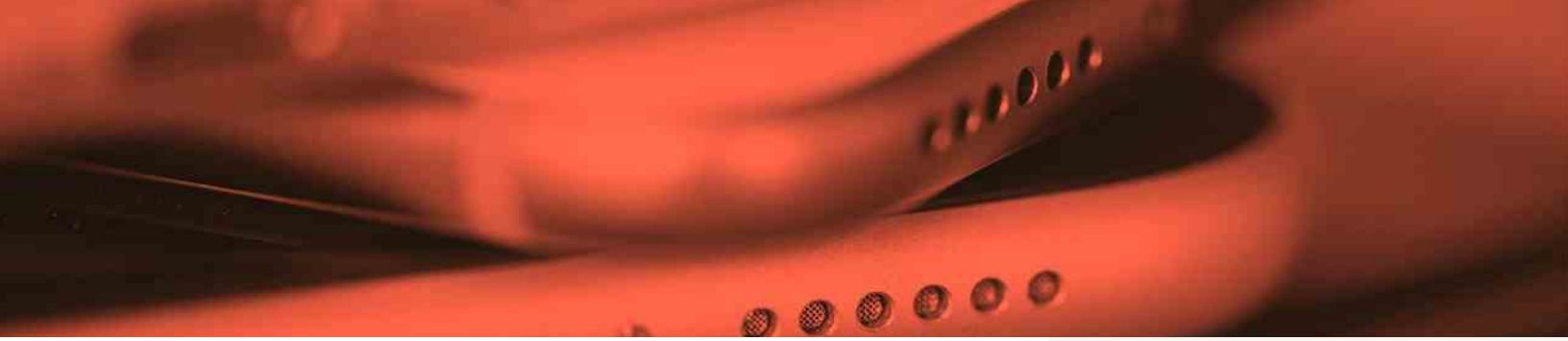


However, what happens once access is granted? What can be done then to curb the data mining of personal information? This is where Apple's App Tracking Transparency framework and Google's Advertising ID policy step in to protect the unauthorized sharing of privacy information gathered from any of the sensors and technologies built-in to mobile devices. Both solutions require developers to utilize them when developing their apps and services, placing control of privacy data squarely into the user's hands.

Moreover, device management solutions such as Jamf Pro adhere to these requirements, allowing IT to designate company apps, not only allowing them to be deployed but also managed securely, while not being able to access or interact with any of the personal apps – nor their data – contained on personal devices that are part of a BYOD model or company-owned devices that are part of a CYOD/COPE model.

By striking a balance between securing apps and data, as well as the device itself, but allowing users to ultimately control the private data associated with their personal apps and device usage, companies can best protect proprietary data that is both sensitive in nature and confidential, while maintaining a "hands-off" approach to personal user data, allowing for end-users to control the level of access to this data, further enhancing the overall privacy protections in place.





Trend 4 — End users still pose the greatest threat to data security

One basic premise regarding security holds true above all else: regardless of the types of security controls in place, their configuration to aggressively monitor, detect, and mitigate risk and despite the level of automation to prevent and remediate security-related issues – it can mostly be undone by a user unknowingly.

This isn't FUD (fear, uncertainty and doubt), but a very real truth about the level of protection put into securing corporate networks with often little to no regard for the training of the user base. Hence why malicious actors continue to thrive by targeting this "low hanging fruit" in their attempts to obtain sensitive data through phishing and malicious/unwanted software campaigns to ultimately breach corporate networks.

There's a saying that identifies security as being everyone's responsibility. This is also true as IT and Security teams may have the skills and tools to implement controls and remediate threats but ensuring the ongoing success of secure practices is something that all users share in, regardless of their role within an organization. And worryingly, there are very basic security measures that are still being overlooked. According to Jamf Threat Labs data, 2% of devices used for work had the lock screen disabled in 2021, down from 3% in 2020. This poses a significant threat if a corporate device is lost or stolen.

According to the FBI's Internet Crime Report 2020, which was published in 2021, the top three crimes reported by victims were (1) phishing scams, (1) non-payment/non-delivery scams, and (3) extortion. Also highlighted in this report: phishing attacks (including vishing, smishing and pharming), impacted 241,342 victims in 2020, up from 114,702 in 2019, with adjusted losses of over $54 billion. Additionally, phishing impacted more than twice as many people as the second biggest crime: non-payment/non-delivery. The consequences of phishing for consumers is bad enough, but when you look at the impact on organizations, it's dire. According to Verizon's 2021 Data Breach Investigations Report, 36% of data breaches involved phishing, 11% more than the previous year.

2% of devices used for work had the lock screen disabled in **2021, down from 3% in 2020**

According to Jamf Threat Labs data, **one third (29%)** of organizations had at least one user fall for a phishing attack in **2021**.

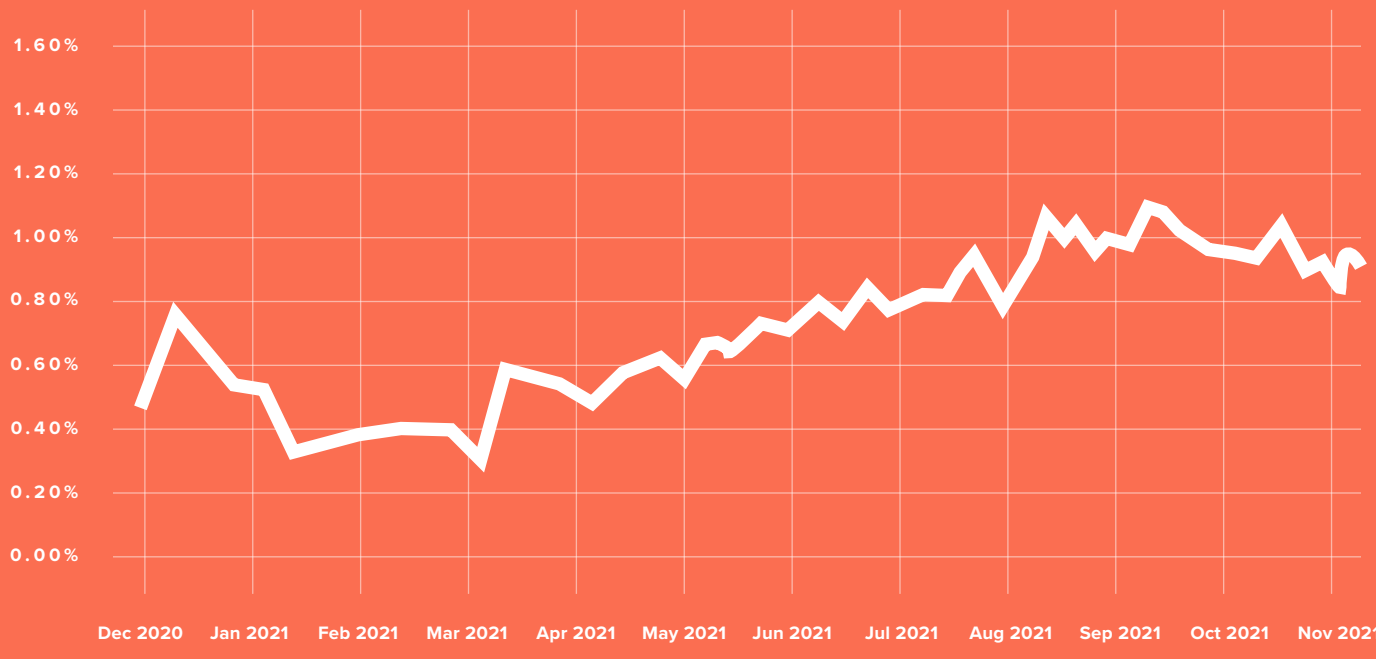
Source: Jamf Threat Labs

Users can also connect to risky hotspots while on the move. The convenience of free Wi-Fi at the airport or coffee shop is often too alluring for employees who may not give a second thought to the potential impact of an attack in which a bad actor uses a Wi-Fi connection to silently intercept a data transfer, known as a Man-in-the-Middle (MitM) attack. But these aren't the only risks present on Wi-Fi. There are a number of indicators of a risky hotspot that could put data at risk, including the presence of a suspicious third-party root certificate that could compromise the authenticity of trusted SSL connections by enabling the interception of encrypted communications.

Over the course of 2021, the number of devices connecting to risky hotspots per week **doubled from 0.5% to 1%**, perhaps due to increased travel and commuting as pandemic restrictions loosened.

Source: Jamf Threat Labs

Devices conecting to risky hotspots per week



Source: Jamf Threat Labs

Devices conecting to risky hotspots per week

Investing in security awareness training programs for company stakeholders is an important part of a company's security strategy and should not be overlooked. This means ongoing, versatile training for end users that covers a variety of best practices and educates users on the latest threats that are most likely to affect them. This will empower them to better identify new and evolving attacks and take proactive steps to improve their security hygiene — not just at work — but also in their personal lives.

Trend 5 — Managing app risk is growing more complex

Apps are the lifeblood of computing. With a reliance on Internet connectivity to drive app usage, cloud-based apps and services offer users a wealth of options to stay productive and enjoy downtime while off the clock, all from the same device. But the growth of malware, combined with poor development and supply-chain attacks can place potentially unwanted and malicious apps on devices that can expose data, leak sensitive information and/or compromise the device, and the enterprise in turn.

Jailbreaking devices to remove their internal security to permit the modification of certain features goes against Apple's SLASA. Accessing third-party app stores that peddle questionable apps that are normally barred from operating in the official Apple and Google App Stores is not illegal – but these activities might lead to the installation of illegal "cracked" apps that don't have a license from the developer. Legality aide, the security risk inherent to sideloading apps is similar to that of jailbreaking, both of which potentially lead to the installation of risky apps that can infect devices with malware, spy on users, steal or leak PII (Personally Identifiable Information), flood their device with ads or brick it outright and worse. According to Jamf Threat Labs data, less than 1% of organizations had one or more jailbroken or rooted devices in their fleet in 2021 and 5% of organizations had one or more devices install a third-party app in 2021.

The internal code of these unofficial or illegally obtained versions of applications is not reviewed nor scanned for security threats like the apps on the official app stores. This means that an app posing as a secure browser alternative, may in fact be malware.

When selecting apps for approved business use, IT teams should ensure they are properly vetted for use with the organization's infrastructure and they should carry out continuous and dynamic app vetting that goes beyond just static code reviews. This will catch issues that arise when the app reaches out to the internet while in-use, such as weak or no encryption ciphers, ad delivery networks that are known to deliver malware, or **unknown or unadvertised "features" that effectively create a trojan-horse-like situation** where an app is used for one function, but secretly permits another function to operate in the background.

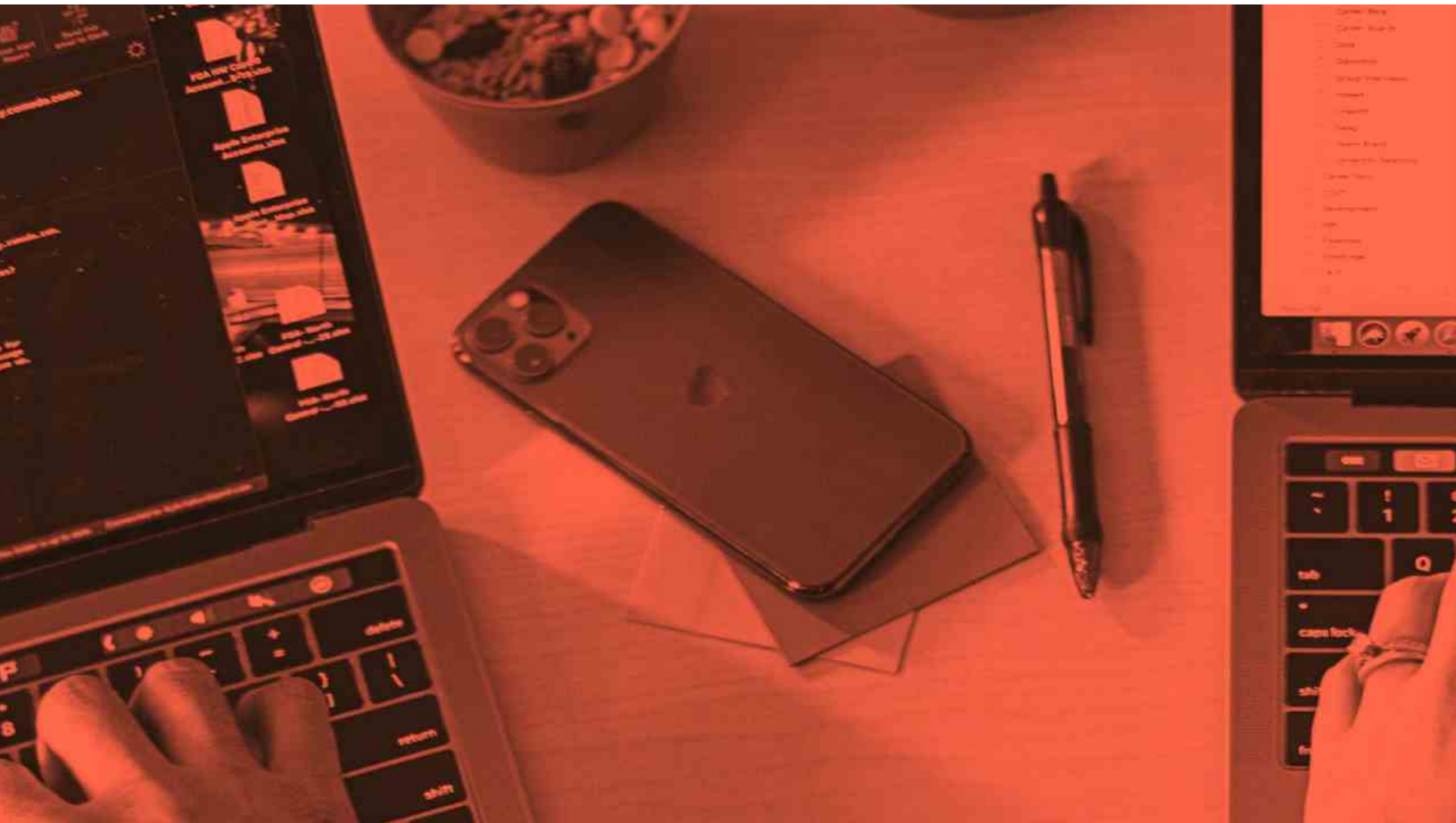
Less than 1% of organizations had one or more jailbroken or rooted devices in their fleet in **2021**

And **5%** of organizations had one or more devices install a **third-party app in 2021**

Source: Jamf Threat Labs

Another significant concern relating to app security is pipeline attacks or those that seek to compromise the distribution or supply channel as a means to indirectly compromise all devices that rely on the compromised app or service. While this form of attack is difficult to identify since it usually occurs against the manufacturer or developer of the app itself, they typically have **deeper impacts with longer lasting effects on the organizations** affected by them, as explained here in a report by CNN on the SolarWinds attack that compromised commercial software used to manage networking equipment back in December 2020 that still plagues organizations today. There are things organizations can do to insulate themselves from this type of exposure as much as possible.

We recommend deploying apps and services only from known developers using the official app stores for your device ecosystem. Testing applications in non-production environments allows IT and Security teams to gauge how the app/service operates, permitting them to make any adjustments necessary prior to final deployment. For organizations that develop in-house apps, ensure your development infrastructure is secured with access limited to only those that require it, such as programmers, and reduce the number of apps running within those test beds to solely what's necessary to develop the app. Following secure app development practices, regular fleet-wide app vetting and keeping the environments updated will help to mitigate many of the factors that permit malware to infiltrate development sites and minimize the likelihood of a third-party compromising the development workflow leading to the development of compromised applications being deployed into production.



Recommendations

Despite a decades-long attempt to define corporate IT standards, many businesses have reached a point where the lack of standardization is the standard. According to the **Verizon MSI** 2021, nearly a quarter (24%) of survey respondents said that their organization had sacrificed the security of mobile devices to facilitate their response to restrictions put in place due to the pandemic. Which OS does your business use? All of them. What type of users do you allow to access your apps? All of them. What locations are users allowed to work from? Any of them. Secure remote access solutions need to be flexible and agile enough that they enable, not block, and not get in the way of productivity. We recommend using this checklist for developing a modern cloud-delivered security strategy to fit the needs of today's hybrid IT environments.

Outline the requirements based on the new use cases that remote work is creating

- What are you trying to enable employees to do on their devices — access email or access sensitive databases? Segment data so access can be granular.
- Evaluate your use cases and define requirements for your remote workforce.
- The above requirements will inform your device ownership model — which device types will you support, who owns them and how are they managed?
- Prioritize end user needs to ensure adoption of security tools – choose solutions that won't slow them down or get in the way, and that work for the device ecosystem they are using.

Provide fast and secure connectivity

- Regarding connectivity and cloud applications, determine what you need to know about users, devices, networks and apps before you grant them access to corporate resources.
- Limit users to only the business tools they need, this prevents privileged accounts being exploited to attack large numbers of systems.
- Adopt continuous conditional access for real-time evaluation of policy.

Define and enforce acceptable use policy

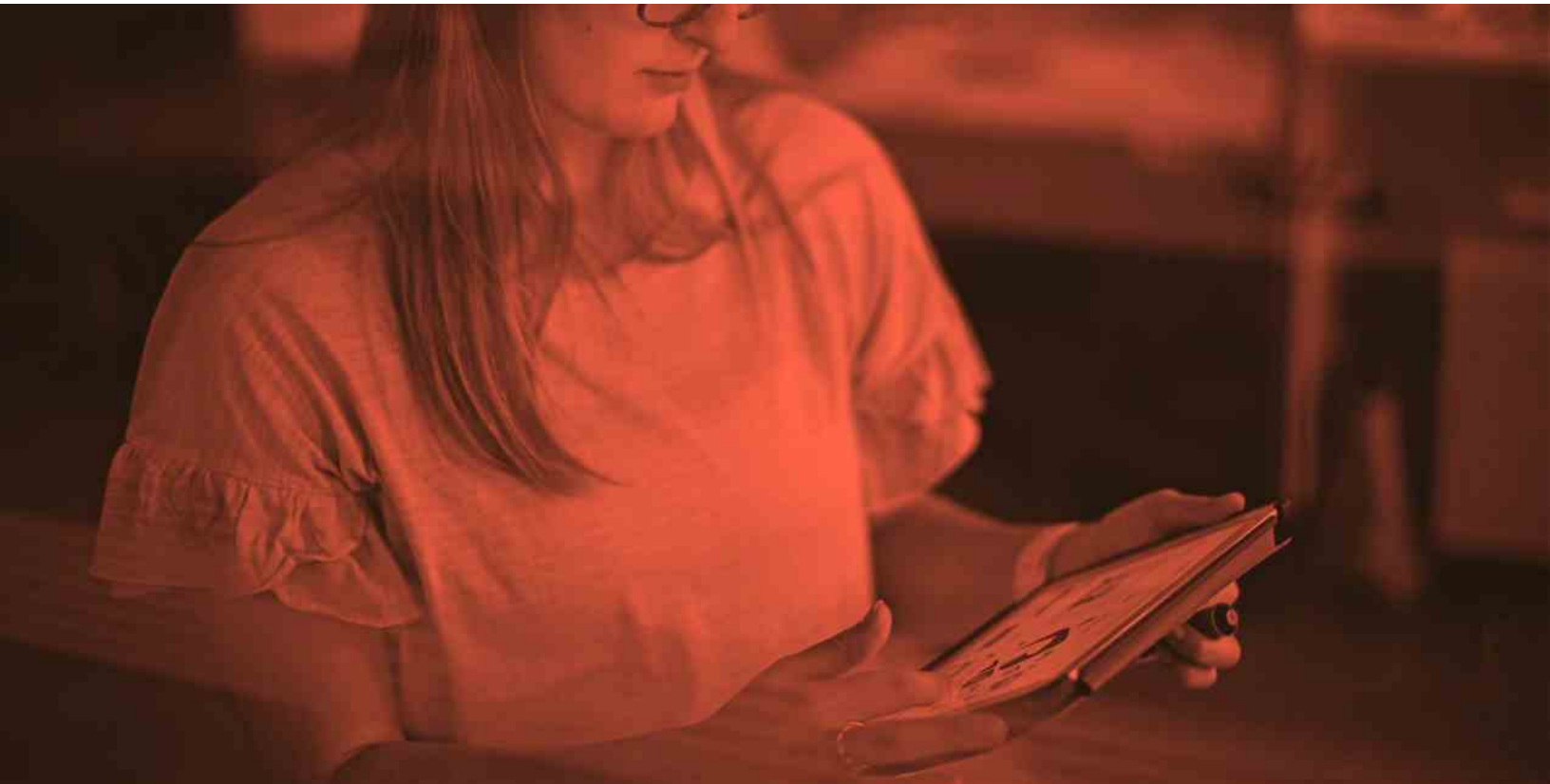
- Review your existing acceptable use policies and ensure that all types of endpoints are incorporated.
- Implement an acceptable use policy for each appropriate subset of devices to control shadow IT, unwanted usage and to ensure regulatory compliance.

Deploy a management solution that is flexible enough to suit all device ownership models

- Deploy a management solution that will enable you to provision devices with corporate resources, configure accounts and connectivity, and undertake ongoing security and compliance checks without over-managing and encroaching on user privacy.
- Automate remediation for devices found to be out of compliance or in a vulnerable or compromised state to bring them back into compliance.

Expand access management policies to incorporate device risk posture

- Implement a user-friendly IAM (Identity and Access Management) solution for authentication to corporate apps on all devices, including mobile.
- Incorporate device risk assessments into your IAM policies to ensure that device risk posture is considered.
- Ensure risk posture is continuously evaluated for the duration of a session.



Deploy endpoint protection across all devices, a cloud-based security solution is especially important for protecting against the broad spectrum of cyber threats and usage risks including zero-day attacks

- Ensure that your security solution has a strong endpoint detection capability with on-device capabilities that are complemented with network-based preventions to stop attacks before they get to a device.
- Ensure that your security solution can address both external cyber threats (like phishing, man-in-the-middle attacks and malware) and usage behavior risks (side-loaded apps, etc.)
- For all security tools, ensure appropriate configurations are made to address the threat vectors that are appropriate to your business while respecting the privacy of your end users.
- Evaluate the security solution's machine-learning capability to understand how the threat engine identifies and protects against new and unknown threats (heuristics/behavioral analytics).

Revisit this list regularly and consider what changes need to be made based on the following

- Changes in company size and composition, eg. mergers or acquisitions
- New regulations that affect the way you handle data
- Evolving IT strategy
- Threats that you have seen affecting employees
- Purchases of new equipment and decommissioning of devices at the end of their lifecycle
- New applications employees need to get their jobs done
- Changes to OS frameworks that govern manageability, deployment and data privacy

About this research

We wanted to better understand the biggest security trends emerging in the new world of hybrid work. The information and statistics found in this paper is the result of our analysis of security trends within a sample of 500,000 devices protected by Jamf, spanning iOS, macOS, iPadOS, Android, and Windows, across 90 countries, over a period of 12 months. This analysis was carried out in Q4 of 2021. The metadata analyzed in this research comes from aggregated logs that do not contain personal or organization-identifying information. Our intention with this analysis is not to invoke fear, but instead to educate you and your users on the options available and how to best keep all aspects of device, user and organizational data secure. **Contact us** to learn how you can put safeguards in place and scale your security posture.