jamf

Cloud Security Report 2021

A close look at the threats that will impact your organization's data via your most critical assets — your endpoints, users, and your remote access tools — plus practical advice on how to configure business tools to ensure fast and safe connectivity for all users in 2021.

Key Findings:

- 52% of organizations experienced a malware incident on a remote device in 2020, up from 37% in 2019; a 41% increase.
- Of devices compromised by mobile malware in 2020, 37% continued accessing corporate emails after being compromised and 11% continued accessing cloud storage.
- In 2020, 28% of organizations were regularly utilizing an operating system with a known security vulnerability.
- Relative to pre-pandemic times, there has been a notable increase of up to 100% in connections to inappropriate content during office hours.
- Android devices were 5.3x more likely to have a vulnerable app installed than iOS devices.
- At their peak during the weekend, phishing attacks were 6% more frequent than during the weekday peak.
- In 2020, 4% of users connected to a risky hotspot each week, down from 7% in 2019, however;
- 15% of organizations had at least one device using an app that leaked password data, up from 11% in 2019.

NOW

Introduction

In 2020, many organizations were forced to transition their business practices to a fully remote model while maintaining productivity levels. As a result, IT policy is being revised to accommodate more devices, more networks, and more apps, in more places than ever before.

The borderless enterprise is here. A Gartner survey of CFOs in March 2020 revealed that 74% intend to shift some employees to remote work permanently.

As a result, we are seeing the old assumptions of good security practices change before our eyes to meet the new normal. The most successful IT operations focus on enabling users while they are away from their desks. This means being more agile and flexible with your security strategy to accommodate the varying needs of a dispersed workforce, and that requires a cloud-first model.

Key industry experts believe SASE (Secure Access Service Edge) will be the key architecture model for innovative companies moving away from traditional technologies, because SASE converges and aligns the functions of networking and security into a unified cloud-native service.

While SASE may be the future, businesses need to find the right tools for the job today. It's important to understand the cyber risks and how they can be introduced to the organization, and that is what this annual report aims to do.

Each year, we analyze the threats impacting mobile devices used for work. As our product portfolio has evolved (to encompass devices beyond smartphones and tablets), so too has our perspective on the mobile workforce — it's a remote workforce, and it involves more than just mobile devices.

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

Risk Factor 1

Endpoints

The introduction of portable devices over recent decades has greatly enhanced our ability to collaborate and share information wherever we are. In 2020, most corporations entered full-time remote work arrangements when their employees were forced to transition to a work-from-home model due to COVID-19.

While it was not a straightforward transition for all, it was for some organizations — particularly for those that were already supporting some full-time remote workers and the occasional work-from-home day for full-time office workers. In many cases, IT had to make some hard and fast decisions about what devices should be allowed or denied access to sensitive business data. This has led to major inconsistencies that perhaps some IT and security teams were not ready for.

More devices + more device types

Over the past decade, people began consuming more and more internet data on their smartphones. The same applies to work-related data, with the rise of mobile SaaS applications, including productivity suites like Microsoft Office 365 and CRM tools like Salesforce. In a typical organization today, 60% of devices containing or accessing enterprise data are mobile.

Before 2020, mobile work was largely about a select few employees on the road staying connected with a smartphone, either owned by the employee (BYOD) or owned by the organization (COPE). Now it's about people who are working full time out of their house or vacation home with whatever device they have on hand, and apparently they have a few options to choose from. Cisco predicts the number of devices connected to IP networks will be more than three times the global population by 2023.

The difference between 'mobile' workers and full-time 'remote workers' is beginning to crystalize. And with that, it is becoming increasingly clear that many of the workflows that employees use are not possible or sustainable from home offices with traditional remote working tools.

Without the budget or supply chain in place to get sanctioned devices to users, many IT teams are allowing employees to purchase and sometimes even choose their own computing equipment to complete their home workstations. This means ultra-portable and convertible form factors with enormous computing power, like a Surface Pro, or a large-screen tablet acting as a second monitor, or a MacBook Pro with a high-resolution monitor or two.

Workers who used to rely on landline phones may have acquired a second smartphone to maintain the boundaries between work and play. It's a buffet of device types, and IT teams have their plates full.

Remote workers are also relying on new portable internet devices that leverage a cellular signal to connect wireless devices when their home Wi-Fi bandwidth is stretched thin. They lean on Verizon Jetpacks, mobile hotspots, and Mi-Fis for multiple portable network options to maintain reliable internet connections throughout and outside of the home.

A wider variety of hardware being used for work introduces a wider variety of software, and as we know well in the security industry, software is subject to vulnerabilities. Many of our customers support a fleet of devices running a combination of Android, iOS, Mac, and Windows 10. And they are trying to standardize a consistent policy across all of these platforms, which is not easy when each platform offers different levels of control and functionality as well as different ways of issuing security patches for vulnerable operating systems.

Industry Spotlight

Generally, public sector devices see fewer threats than others, due to good security practices. However, they often run outdated operating systems, with 4.4x as many users running operating systems with low severity vulnerabilities, and 3.6x running operating systems with high severity vulnerabilities, when compared to global averages.

Lack of device standardization is the new standard

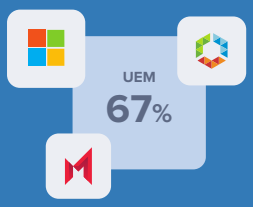
The lack of device standardization is creating new challenges for IT teams. Back when organizations had only one device type to worry about, say a Windows desktop machine, they had only one OS type to worry about. Maybe a handful of those devices were running a few versions behind — let's say up to three versions behind. That meant only four OS versions that IT teams needed to know about and monitor for vulnerabilities. Today, with multiple platforms being the standard – Mac, Windows, iOS, and Android – when you factor in outdated OS versions, what once might have been only four OS versions to worry about now turns into 16 OS versions. The key takeaway is: if you give people choices, you need to be prepared to scale up management to support those choices.

The endpoint security dilemma

Organizations aspire to strong endpoint security, but they run into common dilemmas —such as how to temporarily secure contractor devices while they are accessing sensitive data, or how to respect the privacy of employees on BYOD devices while still enforcing some kind of security. Users are generally opposed to security and management solutions. They do not want to be spied on and they know that these solutions need to conduct monitoring to catch the bad stuff.

We know that 70% of successful breaches originate on the endpoint. We also know that 83% of organizations say that providing access to third parties (e.g., contractors or supply chain partners) is difficult to extremely difficult, so there are improvements to be made when it comes to securing unmanaged endpoints.

According to Verizon, 87% of enterprises are seeing mobile threats outpace other threat types. This is likely because mobile devices are difficult to manage and secure, due to their personal nature, and bad actors are aware of this security gap.



According to our data, 67% of mobile devices are enrolled in a device management software, such as MobileIron or VMware Workspace ONE.

In one study, 92% of FT 500 companies said they were worried that their growing mobile workforce represents a rising risk of security issues. While the majority of organizations have embraced bring your own device (BYOD) policies, the vast majority (94%) said BYOD has increased mobile security risks.

Remote working is likely to remain a part of standard business practices, even after enough of the population has been vaccinated against COVID-19. So IT teams need to establish practices that fit the needs of a broad array of managed and unmanaged devices and networks. They also need to ensure that remote devices are no longer on the periphery of security operations by bringing the threat data together from all endpoints into the SOC.

Risk Factor 2

Users

Operating systems are built to mitigate the vast majority of security threats. Apple and Google have taken great strides to strengthen the security of their operating systems and app stores. However, risks can be introduced by user behavior. To understand user risks, we need to consider how certain attacks exploit user weaknesses. But we also need to consider user behaviors that weaken device security, opening the doors for attacks.

User as targeted victim

Hackers are still getting around hardened operating systems with social engineering attacks like phishing, which aims to target and deceive a user into handing over sensitive information. Users can also have their traffic intercepted by bad actors who leverage the insecure nature of public Wi-Fi. Additionally, users can fall victim to dodgy apps that expose them to data loss events, such as PII or financial theft and other scams.

Phishing

Phishing remains the number one threat impacting users on portable devices. Phishing attacks typically focus on topics, brands or themes that have a high chance of luring victims. For example, each year around tax season, there is an uptick in phishing attacks posing as the IRS, the HMRC (UK), and the ATO (Australia). Likewise, during the first half of this year we identified an uptick in traffic going to COVID-19-related phishing sites, and even the emergence of a fake Clorox e-commerce site.

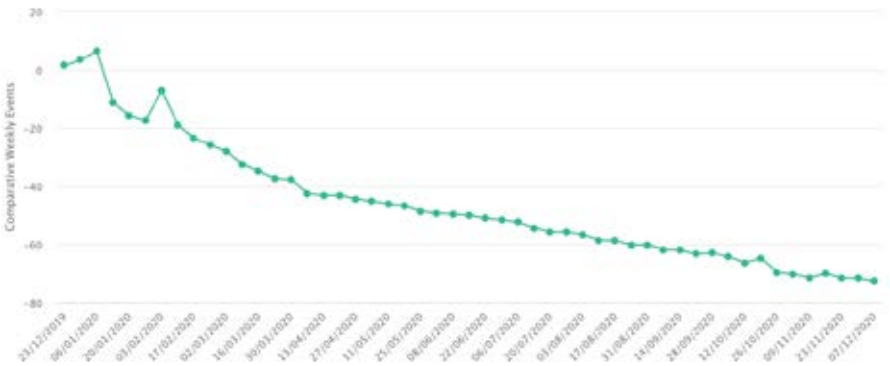
The below chart shows the increase in phishing attacks targeting remote workers over the course of 2020.

While looking for other phishing trends that emerged in 2020, we noticed phishing attacks are reaching users the most on Saturdays. At their peak during the weekend, phishing attacks are 6% more frequent than during the weekday peak. This reinforces the idea that while employees are not in 'work mode,' they are more susceptible to phishing attacks on corporate devices due to being in a relaxed state of mind.

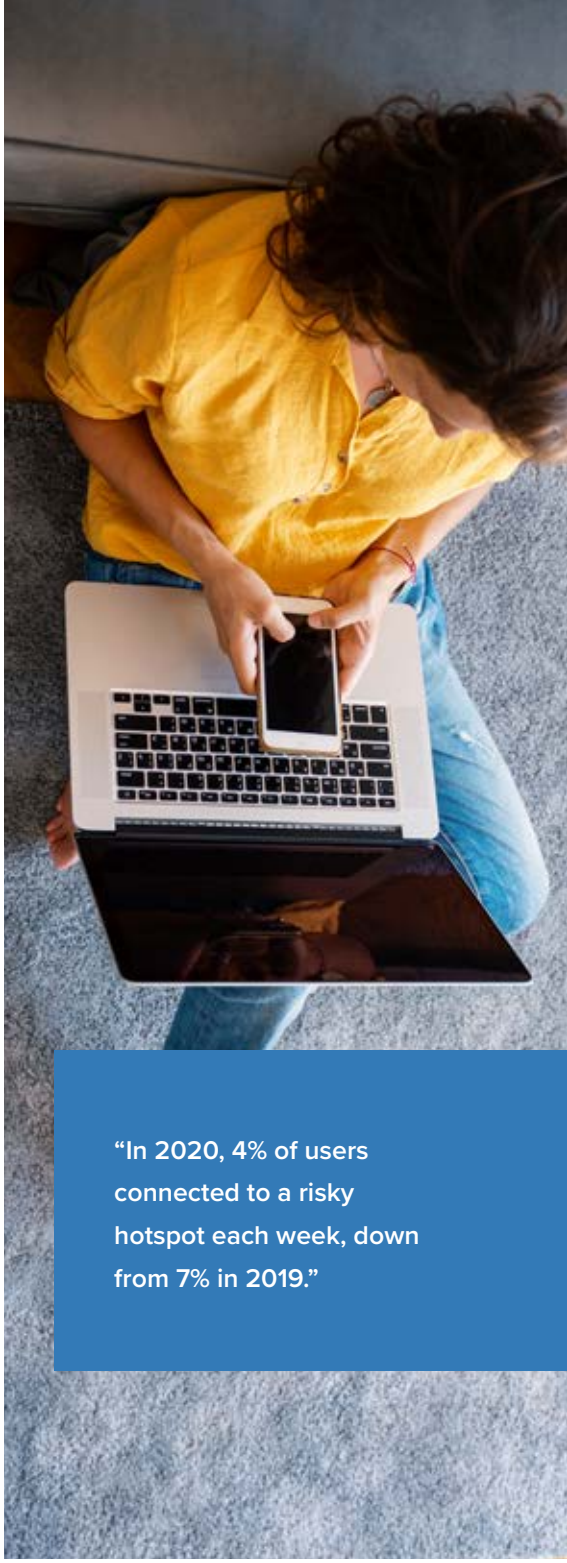
Man-in-the-Middle attacks on Wi-Fi

Wi-Fi presents a serious privacy risk when a Man-in-the-Middle (MitM) attack occurs. There are two primary flavors of MitM attacks that we see impacting mobile users. The first is when the attacker has physical control of network infrastructure, such as a fake Wi-Fi access point, and is able to snoop on the traffic that flows through it. The second is when the attacker tampers with the network protocol that is supposed to offer encryption, essentially exposing data that should have been protected. Alarmingly, more than 80% of employees use public Wi-Fi for work tasks, even when officially banned.

Let's look at how the impact of Wi-Fi threats, including MitM attacks, have changed over the course of 2020.



When we conducted this analysis, we expected to see a decline for one obvious reason — people are not traveling for work as much as they were before COVID-19 took hold (around February – March 2020). In this chart, we see a short uptick in January as people came back to work and then a steep decline in February as COVID-19 case numbers shot up and companies began cancelling work travel and advising employees to work from home in order to keep them safe.



"In 2020, 4% of users connected to a risky hotspot each week, down from 7% in 2019."

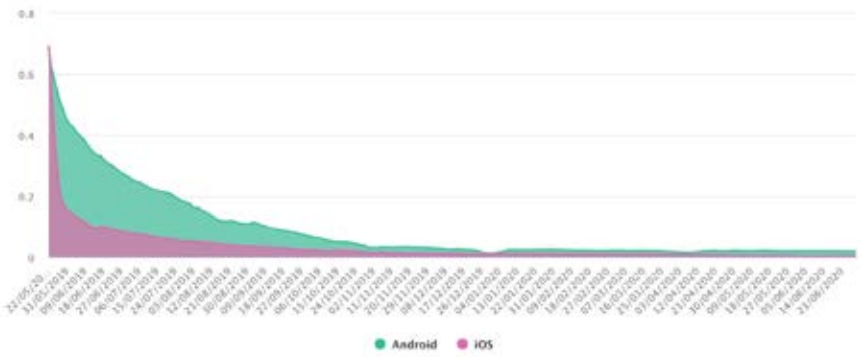
App risk

Malicious apps, such as malware, are increasingly using clever techniques to evade detection. For example, sophisticated malware will wait a certain number of steps before initiating malicious behavior, for example, they will only behave badly on a certain network, or they will contain dormant command-and-control code that can be activated by a hacker at any time. Basic checks, such as those performed by the app stores will not catch sophisticated, but surprisingly common malicious apps.

> **In 2020, 52% of organizations experienced a malware incident on a remote device, up from 37% in 2019.**

Aside from malware being hidden in applications, apps can also just be poorly built, secured, or maintained by developers and therefore subject to dangerous vulnerabilities such as those discovered in WhatsApp in 2019 and 2020.

> **Android users took longer to update their apps after a major vulnerability was found in an older version of WhatsApp in May 2019, as shown in the graph below. From mid May to mid July 2019, around 85% of the remaining devices impacted by vulnerable versions of Whatsapp had updated. Comparatively, only around 50% of vulnerable android devices updated during that time.**



Sometimes apps contain a scam or other fraudulent activity, and often the developers introduce these scams via third-party advertising infrastructure. We've seen apps that have made it through official app store checks despite being full of pop up ads that take over the device screen making it unusable. We call these potentially unwanted apps and 1 in every 200 devices has one installed.

- Some developers may even be careless enough to forgo using encryption and therefore expose the user (and also their employer) to a data loss scenario.
- In 2020, 15% of organizations had at least one device using an app that leaked password data, up from 11% in 2019
- In 2020, iOS devices were 3.2x more likely to be impacted by leaky applications than Android devices
- Our recent analysis shows that once risk is introduced by an unapproved application, the risk compounds.
- with at least one device compromised by malware are 4.4x to be impacted by a password leak than other companies.
- with a vulnerable application installed on their device are 59x more likely to have encountered cryptojacking traffic than other users.

Independently vetting the security of an application is a laborious task, but a necessary one. With more devices than ever before, users have access to a world of applications. The intention might not always be bad. A user might want to use a pdf merger or other file management tool that isn't approved by IT, but this app might carry risk. IT needs to be aware of what apps users are choosing to use for work for two main reasons: (1) they need to be audited for risk, and (2) they need to be assessed from a productivity standpoint, if proven safe and good for productivity, then they should be embraced and protected.

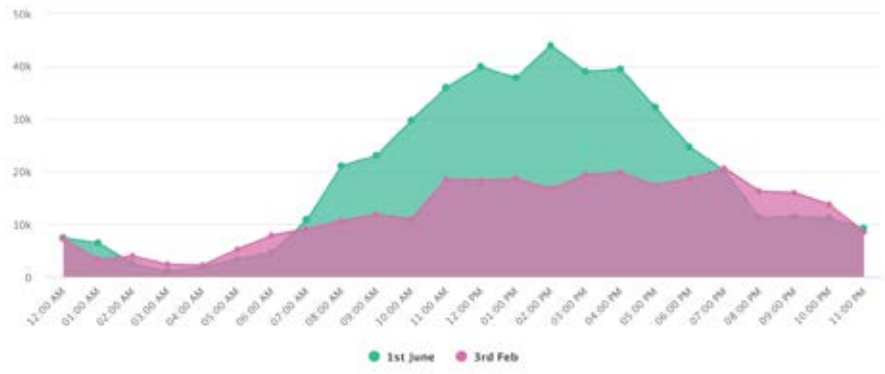
User as bad decision-maker

In the previous section we looked at user-initiated risk with the user in a more passive role. This section will look at user-initiated risk with the user in a more active role, i.e. purposefully circumventing corporate policies and security measures in place. Users can get themselves into trouble with careless decisions, such as accessing non-compliant content, or tampering with their device security such as jailbreaking devices, sideloading applications, or disabling lock screens.

Inappropriate content

Having devices in your IT infrastructure that can access the darkest corners of the internet introduces risk to your business. When we refer to inappropriate content we are referring to the adult, gambling, extreme, and illegal content categories which are far more likely to leak data, employ unencrypted technologies and otherwise expose organizations to risk. Surprisingly, there are many people out there accessing the shady side of the internet using their work devices.

Relative to pre-pandemic times, there has been a notable increase of up to 100% in connections to inappropriate content during office hours. While employees are working remotely, there is an obvious need to ensure that acceptable usage policies are still being adhered to on remote devices.



Content filtering is an effective way to enforce corporate acceptable use policy across a range of endpoints to mitigate security, compliance and legal risks for both employees and their employers.

Circumventing security measures

Vulnerabilities don't always just happen to users, sometimes users make their devices vulnerable, whether intentionally or unintentionally.

Jailbreaking

Jailbreaking and device rooting are risky configurations that allow users to gain access to the operating system of a device and enable the installation of unauthorized software functions and applications. These tactics are also popular among users trying to free their device from a carrier lock.

- In 2020, the number of jailbroken iOS devices increased 50%, while the number of rooted Android devices increased 20%
- Jailbroken devices are 28x more likely to encounter malicious network traffic than non-jailbroken devices.
- Companies who have at least one jailbroken device in their fleet are 31.6x more likely to have devices encountering malicious network traffic than other companies.
- Jailbroken devices are 33x more likely than non-jailbroken devices to have an application with a known vulnerability installed.

In 2019, the number of jailbroken iOS devices increased 50%, while the number of rooted Android devices increased 20%

In 2020, 1 in 10 Android devices used for work contained a third-party app store installed (aka one that isn't Google Play).

Sideloading apps

While some iOS users may jailbreak their mobile devices purposefully to install security enhancements, most users do it to install applications that aren't available on the official app stores. It is also possible to install third-party apps without the device being jailbroken; this is a process referred to as sideloading apps. All the user needs to do is configure the device to trust a specific developer and they can then install any app from that developer without going through the app store. This is how a lot of companies install apps for their employees without publishing those apps on the App Store.

Google does not lock down the Android OS as much as Apple does with iOS. While Android's default configuration does not allow sideloaded apps, it is possible to change settings to allow apps from third-party sources. According to our data, one in five Android users have their devices configured to allow third-party app installs

Users that sideload apps face increased security risks because the application review process enforced by Apple and Google on their official app stores is bypassed and, thus, the device has less protection against inadvertently installed malware.

Disabling lock screen

Surprisingly, one of the simplest security measures available on a mobile device is still often neglected: the lock screen. Despite the lock screen setup being active by default on most devices, some users are going out of their way to disable it, leaving their devices more vulnerable if physical theft occurs. It is also an indicator or poor security hygiene, and our data shows that other threats increase on devices that have this basic security measure removed.

- In 2020, 3% of devices used for work had the lockscreen disabled, down from 6% in 2019
- Users who disabled their lockscreen are 16x more likely than other users to be running an OS with a known vulnerability
- Users with their lockscreen disabled are 2.4x more likely to have their email address leaked than other users

Industry Spotlight - IT Services

Users in IT Services are 2.2x more likely to have their lock screen disabled on their devices compared to global averages.

Risk Factor 3

Remote Access

We've looked at device and operating system risk and user-introduced risk, but what about the risk these things pose to sensitive business applications when remote access is poorly configured or not secured at all? What kind of protection do we need to place between the risky device or risky user and the sensitive data in business applications?

When we talk about protecting business applications, we are not talking about application protection or Mobile Application Management (MAM), we are talking about secure access to sensitive intellectual property within those applications and workloads running in the cloud.

According to the Cybersecurity Insiders Remote Workforce Security Report 2020, 65% of organizations allow workers to access managed applications from personal, unmanaged devices.
Additionally in IDC's Remote Access and Security Challenges & Opportunities report, 40% of cyber breaches actually originate with authorized users accessing unauthorized systems.

Lots of business apps in lots of places

There's one thing we know well in the security industry and that's that surveyed IT professionals have their heads in the cloud. According to survey data in O'Reilly's Cloud Adoption in 2020 Report, 39% of organizations are using a combination of public and private cloud deployments in a hybrid model. Further, in this survey, more than 56% of respondents said they are currently working on or planning cloud migration projects for this year.

What this data tells us that many organizations have adopted – or are in the process of adopting – a decentralized, hybrid environment where data is residing across a diverse infrastructure. Some will maintain control of certain applications indefinitely, but cloud and SaaS solutions have enabled applications to sit outside the corporate perimeter, making access to them a critical area for security services.

Cloud-based applications are favorable in many modern workplaces because they're easy and cost effective for the business to deploy, manage, and maintain; both public and private cloud services have established an acceptable track record, making them viable for businesses of all sizes.

imilarly, SaaS solutions are preferred for certain applications because they completely remove the development requirement and maintenance burden from the organization. There's no question that the reward outweighs the risk when it comes to SaaS; why dig a well when you can just turn on a tap? Gartner has predicted that SaaS solutions will generate revenue close to $105 billion in 2020 alone.

With many organizations moving some apps into the cloud and expanding the number of SaaS apps they use, they are managing more apps than ever before in more places than ever before. Also, according to Okta, the bigger the organization, the more apps it makes use of.

The number of software apps deployed by large firms across all industries world-wide has increased 68% over four years, reaching an average of 129 apps per company by the end of 2018, according to an analysis by Okta. Nearly 10% of businesses had more than 200 apps at the time of the study.

The need for modern remote access

Enterprises used to have one thing they were trying to protect – the data center – and they physically controlled that thing. Legacy remote access tools such as VPN and RDI were built around the foundation of a corporate perimeter and worked adequately when applications were run from the data center. With a castle-and-moat security model, trust is inherent to those inside the network. This means potential attackers could gain access to entire network segments because VPNs and RDIs implicitly 'trust' connections without a robust method for verifying the user's identity or checking the device's security posture.

Why are continuous risk assessments an important part of remote access strategy? Let's let the numbers do the talking.

- Of the devices running a vulnerable operating system in 2020, 1 in 83 were accessing their emails and 1 in 6 were accessing cloud storage at the time of the vulnerability
- Of the devices compromised by mobile malware in 2020, 37% continued accessing corporate emails after being compromised and 11% continued accessing cloud storage
- 42% of companies who have devices compromised by malware have at least one of those compromised devices accessing productivity tools.
- 1 in 200 devices accessing cloud storage have their lockscreens disabled
- More than 40% of companies who have users on vulnerable operating systems have at least one of those vulnerable devices accessing cloud storage.
- 1.3% of customers have a device compromised by malware using productivity tools, including Office 365 and Google Workspace.

So we know that user authentication alone doesn't protect sensitive business data from compromised devices. What's the solution? Zero Trust Network Access is a fundamental shift from the traditional approach. No more boxes, appliances, physical devices. And crucially, cloud-delivered network security is scalable. Without it, you simply can't buy enough appliances to protect all this data moving out of the corporate perimeter and into the cloud.

Additionally, Zero Trust Network Access can carry out continuous risk assessments of the devices that request access to your sensitive applications to ensure the device is compliant, and that might mean a number of things, the device is on a good network, in the expected location, free of infections and vulnerabilities and that the user is authorized to make any given request.

Of the devices running a vulnerable operating system in 2020, 1 in 83 were accessing their emails and 1 in 6 were accessing cloud storage at the time of the vulnerability

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. 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 SASE security strategy to fit the needs of today's 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?

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 over-privileged accounts being exploited to attack large numbers of systems.

Define Acceptable Use

- 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 and unwanted usage and to ensure regulatory compliance.

Deploy a UEM for device-level control

- If appropriate, deploy a UEM solution that will enable you to provision devices with corporate resources and undertake ongoing device compliance checks.

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

- Ensure that your security solution has a strong endpoint detection capability and an in-network architecture to prevent 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, 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 threats.

Revisit this list often 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|
- hreats that you have seen affecting employees
- New applications employees need to get their jobs done

To learn more about how Jamf can safely connect workers to devices app and corporate data, please visit jamf.com