jamf

Security 360:
Annual Trends Report

Introduction

Last year, we looked at how the adoption of remote technologies impacted the security posture of businesses globally. While many organizations were still migrating to remote and hybrid work environments, the focus this year will be on how the threat landscape has adapted and how these trends represent a security risk to your organization from existing threats – and newly evolved ones.

Each year, **Jamf Threat Labs** analyzes the threats impacting devices used in the modern workplace. As the workforce continues to be distributed, our perspective on the modern threat landscape continues to evolve to meet the consistent requirements of endpoint compliance, ensuring data security while upholding user privacy in the face of evolving risk.

This year's report explores five key security trends impacting organizations, with users connecting remotely to a multitude of apps and services hosted in private and public data centers, relying on various cross-platform mobile devices.

2023 Trends address:

1. Social engineering
2. User privacy
3. Novel threats
4. Compliance
5. Workforce distribution

Trend 1 – Social engineering continues to lead the charge as the top threat

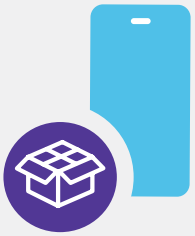
Social engineering, with a specific callout to phishing attacks, is top of the list of significant cybersecurity threats. The volatile mix of a distributed workforce with the relative ease with which bad actors can carry out phishing campaigns leads to successfully obtaining user credentials. Also referred to as "the keys to the kingdom," these attack types grant unauthorized users access to data stored locally within the device. What makes these attacks more dangerous (or impactful) is that they often permit them to pivot access onto other systems as part of their attack chain.

The irony of social engineering attacks is that despite enabling strong security configurations that adhere to industry best practices, many solutions can do little to prevent these types of attacks if users are tricked into handing over their credentials to bad actors, passing themselves off as someone they're not. Making matters worse is how disjointed environments have become, leaving many users without easy access to IT and security professionals when suspicious emails or SMS messages are delivered that seemingly require an immediate response.

Unfortunately, due to the emergent nature of the messages – intentionally written this way to scare victims into clicking a link that steals their authentication tokens, runs malicious code to exploit a vulnerability on their device or simply routes the victim to a bogus website impersonating a legitimate one, tricking them into providing their credentials – the sad fact is that by the time the user has spoken with IT, it's usually too late. For example, **IBM reported** that stolen or compromised credentials were not only the most common cause of a data breach but, at 327 days, they also took the longest time to identify.

Phishing attacks vary quite a bit from other types of attacks, meaning they aren't anonymous actors lying to obtain your username and password. The deception can be made in different ways to yield the same result: take a popular attack carried out wherever public hotspots (see "free Wi-Fi") are available called "evil twin," for example. An evil twin masquerades as a legitimate wireless network, allowing an attacker to effectively steal any relevant data transmitted by the victim without their knowledge, which can be avoided if the device accessing the network is encrypted with a **VPN or Zero Trust Network Access (ZTNA) solution**.

In 2022, 31% of organizations had at least one user fall victim to a **phishing attack.**



In 2022, 16% of users were found to be exposing sensitive data by connecting to **risky hotspots.**

Together, these two data points suggest that:

1. Users tamper with their devices much less than before, and...
2. Bad actors are increasing their attacks on company devices.

Source: Jamf Threat Labs

Statistica estimates that there are currently **432.5 million public Wi-Fi hotspots available worldwide.** And in 2022, 16% of users were found to be exposing sensitive data by connecting to risky hotspots. Assuming that only one user connects to each risky hotspot, that would be 432.5 million users transferring data over untrusted network connections.

The numbers don't distinguish enterprise from personal users, nor do they take into account any endpoint security solutions that may aid in thwarting phishing attacks, such as content filtering software that explicitly prevents access to malicious URLs and domains associated with phishing campaigns.

Most importantly, according to the EC-Council, they don't factor in **the best way to secure your staff.** Whether it's combating social engineering threats or staving off phishing attacks from any number of communications mediums, one of the best defensive measures is not a security control but an administrative one – **cybersecurity awareness training.** With a comprehensive user training program built into your onboarding processes and following up at a regular cadence with frequent updates that are scoped to the very attacks targeting countless organizations globally, users feel empowered with the knowledge necessary to recognize threats and assess risks involved with following through with phishing attempts.

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 implementing 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 identify new and evolving attacks and take proactive steps to improve their security hygiene — both at work and in their personal lives.

The top 10 types of phishing attacks are:

1. **Email:**
   Email messages are sent to individuals pretending to come from a reputable, trustworthy source.

2. **Vishing:**
   Voice phishing attacks switch mediums to a telephone-oriented attack delivery (TOAD), often spoofing the caller's number to pretend to be a trusted source. Like the scam calls claiming to be from the FBI.

3. **Smishing:**
   Like Vishing, threat actors use SMS messages paired with links or attachments instead of phone calls to compromise mobile device users.

4. **Social Media/Angler:**
   New technology gives birth to new attack vectors, hence why these attacks target social media users across various platforms. The latter, Angler phishing, is a newer variation on the social media theme, whereby attackers impersonate customer service staff, often complete with a fake profile account, to target victims requiring assistance.

5. **Spear:**
   A variation of email phishing that instead utilizes a targeted approach, focusing on specific individuals within an organization, like an employee from the payroll department.

6. **Whaling:**
   Similar to spear phishing, this attack refines its scope to target executives and C-suite members.

7. **HTTP/S:**
   Website-based attacks that use URLs that often contain subtle misspellings that may be difficult to catch at a glance, like "iamf.com" instead of jamf.com. It may also include SSL-secured domains that are legitimately registered to bypass the security check features found in modern browsers.

8. **Website Forgery:**
   This attack type often accompanies HTTP/S attacks, pairing a legitimate-looking website alongside the malicious URL, replete with the original text, logos, color schemes and functionality that mirrors the actual website, providing a trustworthy appearance, look and feel.

9. **Watering Hole:**
   Part spear phishing, part tactical, watering hole attacks target specific groups of users and a website they frequently visit. The attack aims to compromise the website, infecting it with malware so that when the targeted users visit the site, they, too, become infected.

10. **Pop-up:**
    Like the pop-up ads of technology yesteryear, this variation on phishing requires bad actors to infect a website with malware, then utilize embedded ads or newer notification alerts enabled by users and infect users when the payload is delivered.

Trend 2 – User privacy has a seat at the security table

While manufacturers and developers, like Apple and Jamf, have been actively banging the privacy drum for some time now. Generally speaking, other technology vendors have historically not held privacy protections to the same level of consideration as other security measures in their hardware and software offerings.

Like the consequences of having personal and business data leaked, the battlefield over protecting user privacy data yields many casualties if violated. Consider that personal data isn't simply gathered without the user's permission. It is being compromised in several ways:

- Nation-states use malicious code that enables tapping communications feeds, like the camera microphone or key-logging on victim devices, to spy on them.
- Bad actors utilize this data for personal or financial gain, as well as to extend social engineering campaigns and to blackmail victims.
- Businesses enrich themselves by selling gathered data without user consent to advertisers and/or third-party partners.

In other cases, organizations that gather personal data as part of their legitimate operating procedures find themselves in trouble due to insufficient protections in place to secure personal data from an external attack, insider threat or regulatory governance. And in some cases, **organizations aren't even aware of the threat,** as evidenced by "5% of organizations having a potentially unwanted application installed within their device fleet in 2022."

At first glance, 5% may not appear to be significant. But evaluating risk goes well beyond just numbers. It takes into account the following:

- Identifying targeted assets
- Any attack vectors present
- Types of possible attacks
- Likelihood of attack occurrence
- Potential impact if exploited or compromised

In essence, combining these allows organizations to assess what risk is present and how it will affect business continuity. How does this apply to personal data?

"**0.4%** of Android devices had a potentially unwanted app installed in **2022** compared to **0.1%** of iOS devices."

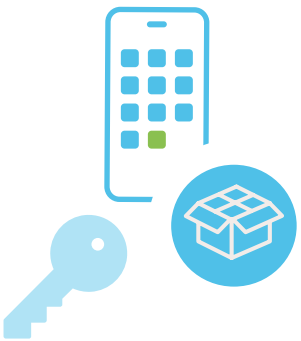
Android is an open ecosystem that results in more risky apps. Apple has created a curated app ecosystem and offers more stringent user privacy protections that limit the introduction of these risky apps.

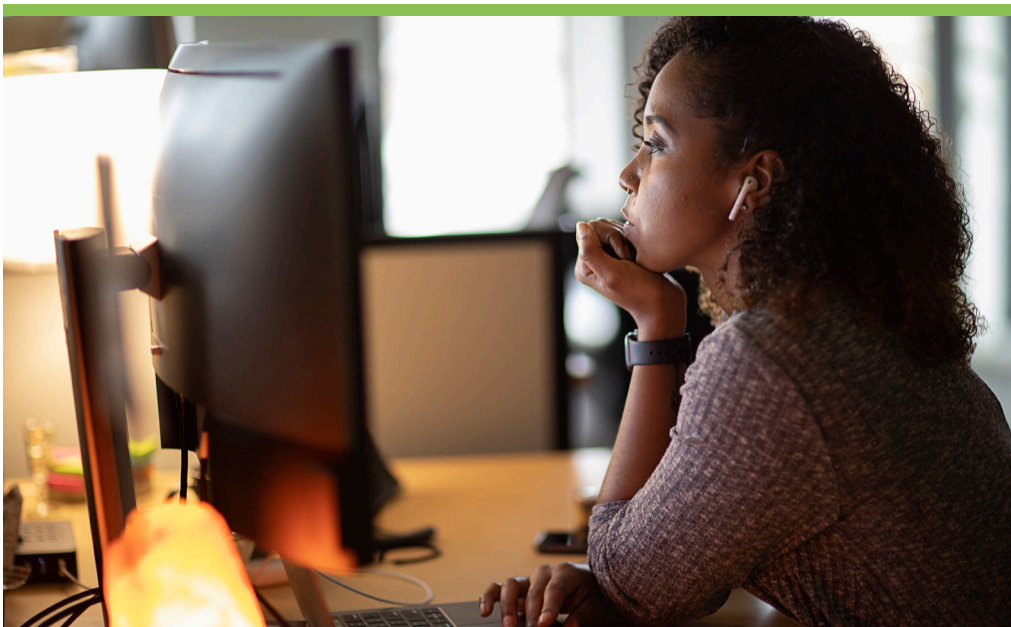
The last point regarding the potential impact if exploited or compromised cannot be understated as it strikes directly at the heart of regulatory controls and how they work to mitigate risks, preventing data leaks that would violate regulatory laws (more on compliance later in this report).

Effective privacy controls continue to gain prominence alongside security controls — not just to enforce compliance where required but also to limit exposing user privacy data as part of the larger security strategy. It must extend to all solutions, processes, stakeholders and workflows within an organization to build overall data security alongside creating or implementing all components across the enterprise — not as an afterthought.

Management solutions help align organizational policies with regulation requirements and lessen the management burden by allowing IT to designate company apps. This ensures that all data types are secured throughout the infrastructure regardless of device type or location.

By leveraging the management of multiple device ownership models, organizations strike a balance between securing apps and data and applying secure configurations to the devices themselves to access business resources securely while allowing users to ultimately control the private data associated with their personal apps and device usage. Companies protect proprietary data that is both sensitive in nature and confidential while maintaining a “hands-off” approach to private user data, **allowing end users to control the level of access** to this data, further enhancing the overall privacy protections regardless of whether devices are part of a BYOD program, company-owned devices that are part of CYOD/COPE initiative or a mix of these models.





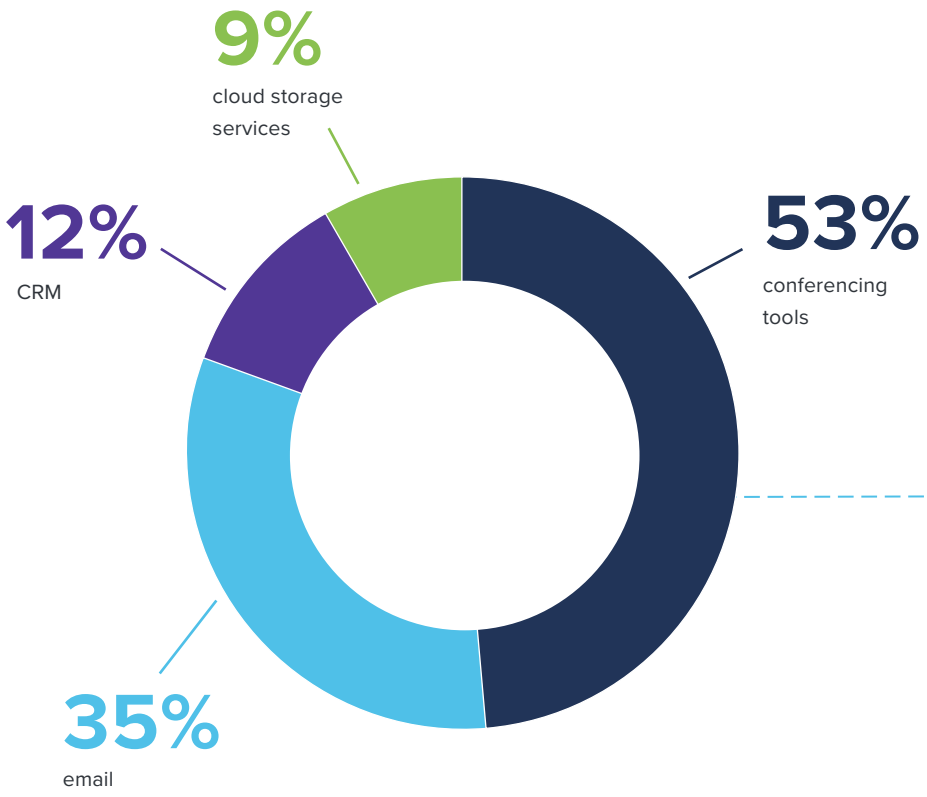
Trend 3 – Bad actors converging attacks into novel threats

Some good news on the macOS malware front — total malware infections showed no signs of growth from the previous year. The better news — in 2022, **new malware infections went down** from just over 150 million to about 100 million infections, according to AV-Atlas' ongoing registration of malicious programs and potentially unwanted applications (PUA).

Malicious network traffic, which refers to network-based Indicators of Compromise (IoCs) that can be observed in the communication patterns between the device and Internet servers, continues to be more prevalent. Malicious network traffic is typically only observed in production environments and cannot be identified by simply assessing static code. That is why actively monitoring endpoint health is so critical when assessing combined risk factors.

Bad actors pairing together various attacks is not new per se; however, the modern threat landscape is seeing more of these converged threats being used actively in the wild to target distributed workforces in new ways to gain unauthorized access to protected services and resources. In a single month of 2022, 53% of compromised devices accessed conferencing tools, while 35% accessed email, 12% accessed a CRM, and 9% accessed cloud storage services.

In a single month of 2022, **53%** of compromised devices accessed conferencing tools, while **35% accessed email, 12% accessed a CRM,** and **9% accessed cloud storage services.**



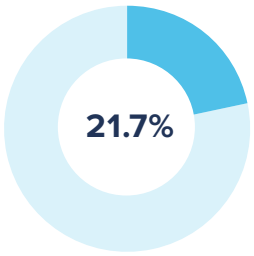
Sophisticated attack example

An employee receives a spear phishing message that appears to be from a colleague. The message includes a link to a "work document," which injects malicious code on the victim's device that gathers their credentials while also delivering a ransomware payload. While ransoming the sensitive data, the attacker uses the credentials to gain greater access to the organization's infrastructure. Finally, the malicious performs two more functions: it adds the endpoint as part of a botnet used to attack other organizations while seeking out other devices to infect, subsequently extending the process and growing the botnet.

The overarching message here is that attacks may take on more than just one form and can occur over any period and often occur without detection. Some attack chains occur shortly after compromise, like ransomware, whereas others are more tactical and require more time, like building a botnet to target systems with denial of distributed service (DDoS) attacks.

This convergence is difficult to protect against since the victims usually don't know the extent of the attack until the next wave begins to impact them. Still, certain practices can mitigate some risks while severely limiting or alleviating the impact felt by others. Actively monitoring endpoints and gathering telemetry data on endpoint health status is a critical bit of data for administrators as it provides deep visibility into devices and how they fare concerning several vectors, like patch levels, especially since suspicious behaviors that may indicate a device is compromised without being seen or felt by an end user.

Speaking of patch management, managing the app lifecycle is table stakes when mitigating risk from system vulnerabilities while ensuring that apps have the greatest level of security in place to protect against known threats. This is especially important when noting that third-party app stores often provide versions of legitimate apps that contain malicious code, infecting user devices. Imagine the free versions of paid apps as bait to lure in victims, for example.



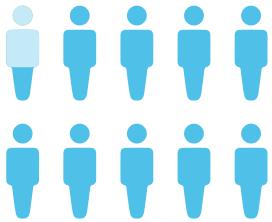
21.7% of Android devices accessed third-party app stores compared to **0.002%** of **iOS devices.**

Third-party app stores are a common way to subvert app review process that protects devices and users.

0.02% of Android devices were rooted and **0.001%** of **iOS devices** were **jailbroken** in 2022.

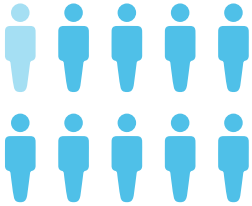
Despite the small percentage, it's notable that the impacted Android device count is twice that of Apple. And if you think about the abstract amount of Android and Apple devices in the world, the scale of this is not hard to imagine.

While specific operating systems (OSs) allow side-loading applications, others, like iOS, require that devices first be jailbroken to defeat the protection that keeps iOS-based devices safe against running unsigned code. Locking down devices is only part of the equation. It is crucial to identify jailbroken devices in real time in order to effectively remediate this threat vector.



0.004% of users and **0.3%** of organizations had a **jailbroken** or **rooted** device in 2022.

Last year's stat:

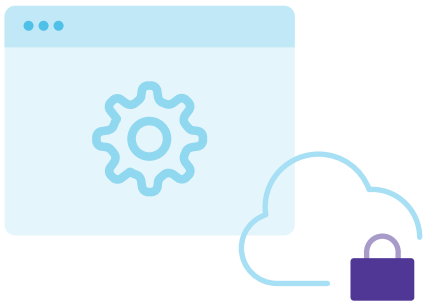


Less than 1% of organizations had a **jailbroken** or **rooted** device in 2021.

Supply-chain attacks

Attacks against the supply chain or **third parties** have historically felt broader impacts that go several layers deep into – and through organizations in the pipeline – before reaching **the attacker's true target.** Its effects are often far-reaching, impacting businesses globally regardless of the strength of their security posture.

Preventing these attacks is a tricky proposition, mainly because organizations lack the authority to require each organization (or their contractors) in the pipeline to mitigate risk factors meaningfully. Sadly, the same goes for protecting your organization against these threats for the same reasons. But as the Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST) point out in their joint technical document **Defending Against Software Supply Chain Attacks**, a key element to "bolster an organization's ability to prevent, mitigate, and respond to such attacks" is to observe industry best practices as part of a comprehensive defense-in-depth security strategy that includes vetting supplier's security processes through independent, third-party auditors to verify that your partners (and subsequently, their partners) are taking the proper mitigation steps before an attack has occurred.



Trend 4 – Complying with regulations is part of the security stack

A growing trend, alongside organizational data security, is the importance of user privacy. This is most prevalent with compliance, particularly with state, federal and regional regulations. Consider how General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) make greater inroads in protecting users' rights to privacy at the country and state levels respectively or how fintech – among the most highly regulated industries globally – is subject to multiple facets of governance.

Here are a few examples of how multiple regulatory laws work either as standalone or in conjunction with another to achieve regulatory compliance in certain industries:

Sarbanes-Oxley Act of 2002 (SOX): dictates specific terms for accounting practices

Gramm-Leach-Bliley Act (GLB): addressing the minimum levels of cybersecurity protection required to maintain information security

Financial Industry Regulatory Authority (FINRA): explicitly details how business processes relate to ensuring the protection of investors through fair and honest operations within the securities industry

In light of compliance regulations impacting businesses in select industries and their global reach, requiring affected organizations to comply with laws that may be well outside of their jurisdiction, organizations find themselves needing to exercise greater control over workflows to uphold privacy and the management of protected data types — like personally identifying information (PII), protected health information (PHI) and business intelligence information (BII) —as it is collected, processed, stored, modified, shared and destroyed following user wishes and/or regulations.

Complying can be a difficult task that requires serious consideration, management and support, even if your devices and data are managed by the organization. But what about enforcing compliance across a distributed workforce that must be able to access organizational resources from anywhere, on any device and at any time? The added complications of on-prem and remote/hybrid workforces can be a pain point for organizations with compliance requirements and are navigating the modern threat landscape.

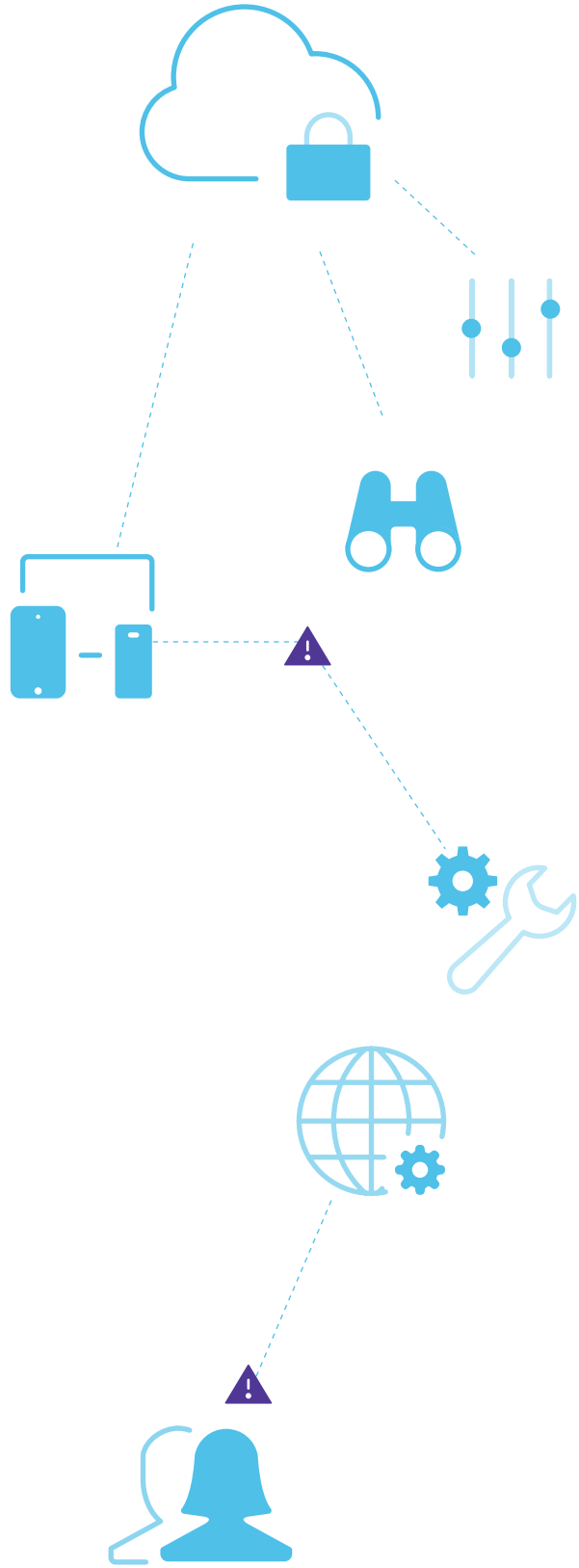
"In **2022, 21%** of employees were using devices that were **misconfigured,** exposing them to **risk."**

Unfortunately, the compliance waters only get murkier when adding personally owned devices into the mix. In 2022, 21% of employees were using devices that were misconfigured, exposing them to risk. More to the point, leaving data that could be sensitive, confidential or mission-critical – and potentially regulated – at risk of exposure, in turn exposing the organization (and possibly the user, as well) to civil and/or criminal liabilities if violations to regulatory laws are determined to have occurred as a result.

While many organizations have implemented some form of BYOD or employee choice program, allowing endusers to select which device types and operating systems they feel most productive and comfortable using, the solution to effective compliance management cannot only be locking all devices out except for managed ones. **We saw that 8% of users and 21% of organizations were impacted by configuration vulnerabilities**, meaning that even company-owned and managed devices can be impacted. Solutions must take more into consideration to respond to security issues beyond device management.

The fact is that any endpoint at any time could conceivably miss a patch, leak data due to a commingling vulnerability or simply be lost or stolen. In each scenario, a different action would be required to mitigate risk. Some situations could be handled via automated response and remediation workflows, but the point remains that there will always be a place for manual remediation as well.

As with most security-centric discussions, there are no silver-bullet or one-size-fits-all solutions that will cover all the bases necessary to keep your infrastructure compliant all the time. We recommend implementing a defense-in-depth security strategy that provides multiple converging solutions to address your unique compliance requirements from many angles.



Trend 5 – Securing data in remote/hybrid environments still poses challenges

The shift to a remote workforce ushered in change for securing users, data and devices. With the network perimeter effectively eroded, on-premises solutions were replaced with cloud-based solutions to distribute security services to users working on any device from anywhere. The result was an endpoint security solution that was more capable and self-sufficient with added resiliency and robust application security.

And yet, despite the identified benefits, organizations are still experiencing challenges to data security from remote and hybrid work environments several years post-migration. Unfortunately, no clear issue points to the culprit. An amalgamation of issues contribute to inadequately securing data. Some of these issues stem from a lack of:

- Real-time visibility into endpoint health
- Integration between management and security tooling
- Automated processes and workflows
- Decentralized logging and threat intelligence
- Policy and compliance enforcement
- End-user security training programs
- Best-of-breed solutions
- Risk assessment practices to identify assets and threats

For example, we found that **64% of vulnerable devices accessed collaboration tools while 34% accessed enterprise email.** This indicates that, while risk and compromise indicators are subjective and will vary from business to business, routine tasks such as patch management are not occurring on all devices. This leaves the devices themselves at risk and puts organizational resources at risk too. It even goes beyond apps and configurations. Jamf Threat Labs found that **1 in every 5 devices ran an operating system that was not up to date.** It's essential that security exists at all layers of a defense-in-depth strategy, starting at the OS level, for protecting users and organizations.

This further drives home the real-world need for visibility into your device fleet and how it interacts with your organization's infrastructure, especially if your industry is regulated. This requirement is furthered when considering that most regulatory agencies require that organizations prove compliance through regularly scheduled audits conducted by regulators looking to verify that protected data and the endpoints that interact with it are secured in accordance with regulatory governance.

But assessing the assets and threats that impact your organization and the accompanying telemetry to identify affected endpoints is just a part of the solution. Modern solutions are needed to mitigate risk and enforce real-time access decisions. Legacy technologies, such as VPN for securing remote connections, certainly can't compete with newer technologies designed to address the challenges of distributed workplaces and the modern threat landscape. 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 safely and securely.

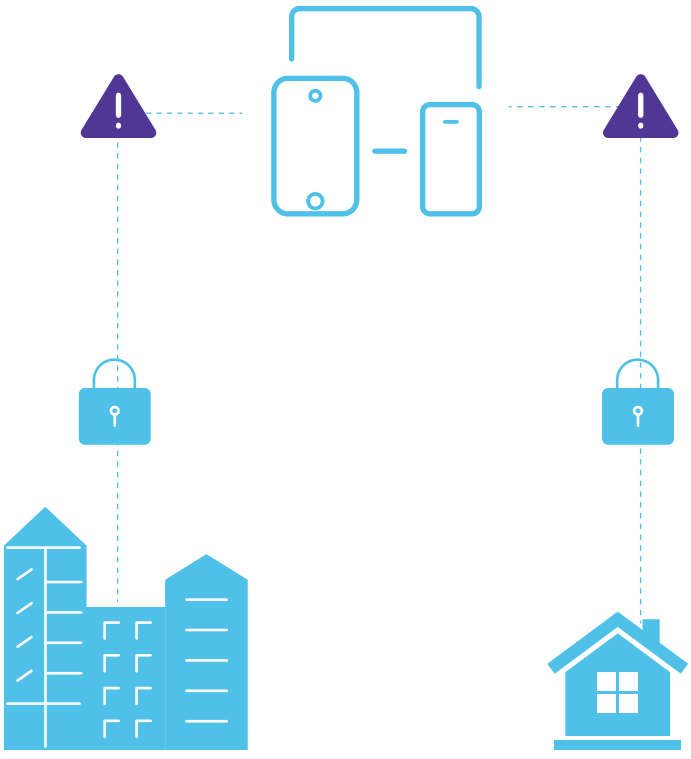
Designed with modern networks and workflows in mind, ZTNA solutions mitigate risk and safeguard data while being flexible enough to ensure that personal apps and data remain private. Beyond that, authorized users only have access to connect to the apps they are allowed to access following the principle of least privilege while routing business traffic through micro tunnels, which prevents attackers who compromise a single user from accessing all the applications the user is authorized to access. Through built-in segmentation of traffic tunnels, attackers are prevented from performing lateral movements throughout the network, effectively limiting threats.

Another key piece is securely integrating solutions by leveraging APIs to share critical telemetry and endpoint health data with solutions that limit the success rate of threats to devices, users and sensitive data. This is in stark contrast to “bolt-on” or standalone solutions that see off-the-shelf security tools working independently but lack the integration component that drives a holistic, defense-in-depth solution.

As bad actors evolve their tools, so must organizations leverage their solutions to prevent known attacks while mitigating risk from new ones. With the latter in mind, threat hunting continues to grow and flourish within organizations, aiding their IT and Security teams in identifying, mitigating and remediating against unknown and novel threats before they can lead to data breaches. Artificial Intelligence (AI) and Machine Learning (ML) technologies have shown their effectiveness in several industries, and cybersecurity is one such in that solutions are increasingly leveraging the expanded processing power and behavioral analytics capabilities to learn, efficiently predict and counter threat actors and their attacks at speeds with which human administrators simply cannot compete.

Center your strategy around mobile device management (MDM) to secure both personal and company-owned devices and keep patches up to date. Deploy endpoint security to prevent malware while gathering rich telemetry data through active monitoring of endpoints. An API is a great way to securely share threat intelligence data between these two solutions and permits organizations to uphold compliance requirements through policy-based enforcement. Adding identity and access management solutions centralize credential management and provisioning of permissions to approved organizational resources while adding multi-factor authentication (MFA) to secure access.

This integrates with modern security solutions, like ZTNA, to secure connections over any network, incorporate ML to hunt for novel threats, stop attacks before they can begin and replace legacy VPNs with modern solutions that segment access requests to mitigate against network-based threats. And ultimately, collect all relevant threats and device health status in real time to holistically automate the device lifecycle management.



Recommendations

As we approach the three-year mark since the global pandemic led to a drastic change in global work environments, the focus for many has shifted from **“how do we continue business operations?”** to **“how do we keep remote users and organizational resources continually protected?”**

One of the key reasons for the shift in mindset is that, despite being remote for several years now, IT and Security teams are supporting over double the number of remote users today (46%) as they were pre-pandemic (21%), according to **The State of Security 2022 report** by Splunk. Splunk’s global research found that “not only are we continuing to see more attacks, we’re also seeing more actual breaches.”

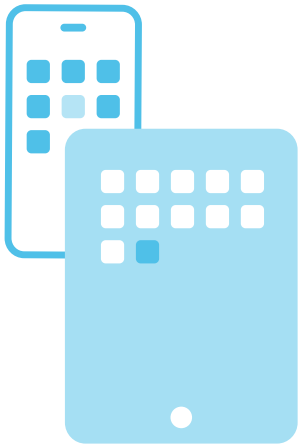
This combination of increasing attack figures, evolving threat landscape and growing need to secure resources accessed by remote users underscores the statement made in last year’s Security 360 report:

> Secure remote access solutions need to be flexible and agile enough that they enable, not block, and not get in the way of productivity.

This year we append to that statement by adding:

> Endpoint security needs to provide convergence of security solutions, leveraging a strong foundation and granular visibility with advanced technologies, like ML, to develop automated secure workflows that serve to align with organizational policies and industry regulations.

Ultimately, organizations should develop a modern, cloud-delivered defense-in-depth security strategy to address their unique needs today while providing the scalability to support the needs of tomorrow.



About this research

We aim to identify the biggest security trends emerging in the new world of hybrid work. The information and statistics found in this paper are the results 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 2022. 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.