ZIMPERIUM.

Gartner Peer Insights.

2022 Mobile Threat Landscape

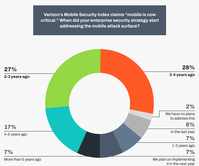
Whether corporate-owned or employee-owned, the number of mobile endpoints continues to grow as, in parallel, mobile applications proliferate to drive growth and productivity for countless organizations and their employees. As this ecosystem spreads, the risks and attack surface expand too. How have organizations traditionally addressed mobile security, and what changes are they making in light of recent publicized breaches?

Zimperium used Gartner Peer Insights to survey 250 IT security leaders to explore the mobile threat landscape in both bring your own device (BYOD) and corporate-owned mobile endpoints.

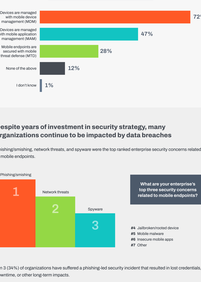
Data collection: October 25th - November 29th, 2022
Respondents: 250 IT and security decision-makers from organizations that have enabled mobile access to enterprise data.

IT and security decision-makers have been addressing the mobile attack surface with mobile device management for years but are behind when it comes to combating contemporary and modern threat types, against which mobile device management is woefully insufficient

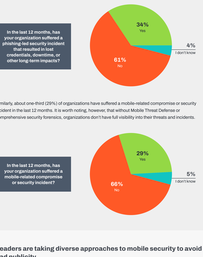
Just over half (52%) of respondents report that the majority of mobile devices at their organizations are corporate-owned/managed devices.



55% of organizations began addressing the mobile attack surface between two and four years ago, which reflects the rise in attacks against mobile devices through critical vulnerabilities, exploitable apps, and unsecured devices. The Verizon MDI report highlighted the adoption of mobile into corporate services as the pivot to the "mobile is now critical" mindset.

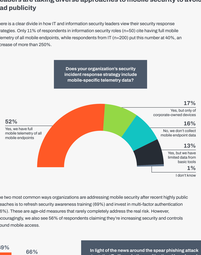


The majority (72%) of leaders cite using mobile device management (MDM) as their organization's infrastructure for securing mobile devices. **However, only 28% reported that mobile endpoints were secured with mobile threat defense.**



Despite years of investment in security strategy, many organizations continue to be impacted by data breaches

Phishing/smishing, network threats, and spyware were the top ranked enterprise security concerns related to mobile endpoints.

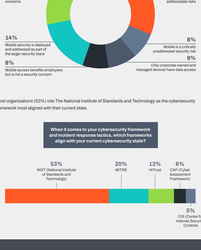


1 in 3 (34%) of organizations have suffered a phishing led security incident that resulted in lost credentials, downtime, or other long-term impacts.

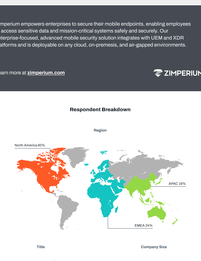
Similarly, about one-third (29%) of organizations have suffered a mobile-related compromise or security incident in the last 12 months. It is worth noting, however, that without Mobile Threat Defense or comprehensive security forensics, organizations don't have full visibility into their threats and incidents.

Leaders are taking diverse approaches to mobile security to avoid bad publicity

There is a clear divide in how IT and information security leaders view their security response strategies. Only 17% of respondents in information security roles (n=50) cite having full visibility and telemetry of all mobile endpoints, while respondents from IT (n=200) put this number at 40%, an increase of more than 200%.



The two most common ways organizations are addressing mobile security after recent highly public breaches is to refresh security awareness training (69%) and invest in multi-factor authentication (66%). These are age-old responses that rarely completely address the root risk. However, encouragingly, we also see 56% of respondents claiming they're increasing security and controls around mobile access.



For 39% of IT and security leaders, ensuring data is securely stored and transmitted is their top security concern when it comes to mobile applications, with evaluation of SDKs just after at 32%. Just 2% do not conduct any risk assessment.

Most organizations view mobile devices as an addressable risk

The most common way leaders view mobile endpoint is that it is a limited but addressable risk (34%), or that they rely on management tools to handle security concerns (27%).

Most organizations (53%) cite The National Institute of Standards and Technology as the cybersecurity framework most aligned with their current state.

Zimperium empowers enterprises to secure their mobile workforces, enabling employees to access sensitive data and mission-critical systems safely and securely. Our enterprise-focused, advanced mobile security solution integrates with UEM and XDR platforms and is deployable on any cloud, on-premises, and air-gapped environments.

Learn more at **zimperium.com**

ZIMPERIUM.

Respondent Breakdown

Gartner

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner. Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, Mobile Threat Landscape survey