2025 Mobile Security Index

verizon business

About the cover

The Verizon 2025 Mobile Security Index (MSI) cover depicts the intersection of artificial intelligence (AI) and human decision-making now shaping mobile security risks. A human hand reaches toward a mobile phone, while an AI hand waits on the other side, representing bugs, deepfake masks and other symbols of emerging AI-enabled threats.

This visual reflects our central theme that mobile device security is increasingly influenced by AI-driven threats and persistent human error. As organizations expand mobile device use, the dual forces of artificial intelligence and human fallibility can open new attack surfaces and magnify risks. Strengthening defenses against evolving threats targeting mobile devices is essential to safeguarding operations, data and trust across all organizations.

Who should read this report?

Mobile security is a challenge that cuts across geographies and organization sizes. A breach that begins with a single compromised mobile device can ripple into lost productivity, regulatory fines, reputational damage and costly recovery efforts. As mobile adoption accelerates—and employees continue to rely on personal devices for work—the stakes for managing these risks get higher.

This report is written for the leaders who must anticipate and manage mobile security challenges. Chief information security officers (CISOs), IT and security directors, mobile program managers, and compliance officers will find data and guidance directly applicable to their responsibilities. Business executives, procurement specialists and policymakers will also gain a clearer view of how mobile security can affect resilience, operations and trust.

In this report, you'll learn how your peers are addressing mobile security, lessons learned from organizations that have implemented effective defenses, and practical insights into the policies and technologies that help deliver stronger outcomes.

About this report

We produce the MSI each year to provide a clear, data-driven view of how organizations are experiencing mobile security risks and how they are responding. Unlike industry headlines that focus on the latest breach, this report pulls together survey data, partner insights and real-world practices to present a broad picture of mobile security across sectors and regions.

Now in its eighth edition, the MSI is designed to help decision-makers cut through complexity and understand where to focus their limited time and resources. The report highlights where organizations are making progress through smarter training, stronger policies and targeted investments. It also shows where gaps remain.

The MSI offers perspective on which approaches—from mobile device management (MDM) to automation and policy enforcement—correlate with fewer incidents and better resilience.

Findings are based on a 2025 survey of 762 professionals across small, medium and large businesses, as well as Public Sector organizations. Additional insights from leading security providers Check Point Software Technologies Ltd., Ivanti Inc. and Lookout Inc. also contributed to the report. The result is a comprehensive source on mobile security trends and practices.

Readers can use this report to benchmark their organizations against peers, identify which measures yield the greatest impact, and inform conversations with executives, boards, regulators and partners. The MSI is not just a snapshot of where mobile security stands today—it is also a guide to where leaders should focus next.

Table of contents

Introduction: AI-driven risks are reshaping mobile security

Every era of technological change has its inflection point. Electricity, the internet, cloud computing – each transformed how people live and work, ushering in new opportunities alongside new vulnerabilities. Artificial intelligence (AI) has reached that moment, collapsing decades of adoption cycles into months.

The Verizon 2025 Mobile Security Index (MSI) finds that for organizations, this acceleration is playing out visibly and urgently on mobile devices. Generative AI (genAI) has quickly become another app on a mobile device home screen, nestled among messaging, productivity and social platforms. Its convenience can disguise risks, introducing vulnerabilities as seamlessly as it enables efficiency.

At the same time, the longstanding challenge of human error remains ever-present. Despite security policies, awareness training and tools, humans still have the tendency to click, trust and take shortcuts that generate risks. The key difference now is that AI appears to sharpen and scale those mistakes, giving attackers the ability to mirror human communication and exploit human behavior with unprecedented precision.

Taken together, the survey findings reveal a perfect storm taking shape. Nearly all employees use mobile devices in organizations of all sizes, and with that usage comes typical human error. Combined with sophisticated, AI-driven attacks, these forces are converging to reshape the risks today's organizations face. Small missteps, such as clicking a single link, can create waves of operational disruption, data and financial loss, and reputational damage.

For security leaders, these challenges are not just about weathering the storm. They are about anticipating the storm's trajectory and understanding what's needed to ensure strong defenses are in place before the next cybersecurity onslaught.

This year's MSI explores how organizations are experiencing and responding to the combined impact of AI-driven threats and persistent human error. The findings make clear that the storm is not on the horizon – it's here, reshaping mobile threats across every industry, organization and geographic location. Our survey findings show that organizations are responding with increased mobile security investments, stronger employee training programs and adoption of key technologies to help defend against these growing risks. Our findings also show, however, that there still is limited use of key defenses and significant gaps exist.

AI and human error: A perfect storm

A perfect storm is brewing as AI powered attacks grow and human mistakes persist.

AI is giving attackers new ways to expand their reach, while human mistakes remain a common entry point for compromise.

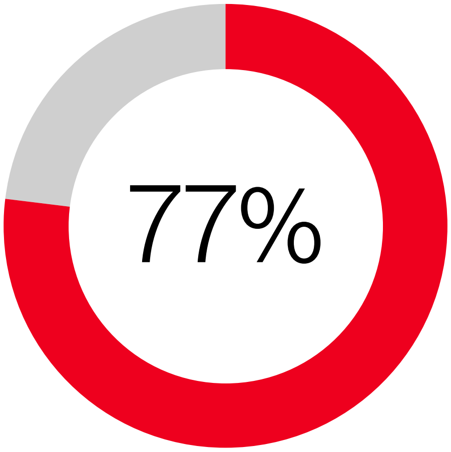
This year's survey data shows how these forces are converging into a perfect storm: Organizations report concern over rising AI-powered attacks as well as high levels of phishing and smishing attempts against employees. Meanwhile, employees continue to click on suspicious links and enter sensitive data into unapproved genAI tools.

AI's rising impact on mobile device security

Mobile device attacks are on the rise for a majority of organizations, as cited by 85% of MSI survey respondents, regardless of their size, industry or location. According to research from Lookout, more than 4 million mobile-focused social engineering attacks were detected in 2024.[1]

In response, three in four organizations have increased mobile device security spending in the past year. While the causes of successful attacks vary, two factors are of particular concern for organizations surveyed: the use of genAI and user behavior.

AI is giving attackers new ways to expand their reach, while human mistakes remain a common entry point for compromise.



77% of organizations believe AI-assisted deepfake and SMS phishing attacks are likely to succeed.

Figure 1: Organizations that view AI-assisted attacks as likely to succeed

[1] "Lookout Mobile Threat Landscape Report - 2024 in Review," Lookout, Apr 9, 2025. https://www.lookout.com/threat-intelligence/report/2024-annual-mobile-threat-report

AI makes attacks more sophisticated.

AI is reshaping mobile threats in ways that draw concern from organizations surveyed. Of respondents, 34% say they fear that the increasing sophistication and scale of AI-powered attacks will significantly raise their exposure, and 38% say ransomware will become even more dangerous when powered by AI. In addition, 77% of respondents believe AI-assisted attacks involving deepfakes – AI-generated media that mimic real people to deceive or impersonate them – and short message service (SMS) text phishing are likely to succeed.

Key mobile security terms

AI-assisted attack

An attack using AI to generate and scale phishing, smishing or malware campaigns

Deepfake

AI-generated media that mimic real people to deceive or impersonate

Phishing

Fraudulent emails or messages that trick people into revealing information or clicking malicious links

Smishing

Phishing delivered through SMS text messages

Social engineering

Manipulating people into giving up sensitive data or access

Zero-day exploit

An attack exploiting a software flaw before a fix exists

Significant gaps exist.

Amid these issues, defenses remain limited.

The limited use of defenses points to uneven progress in preparing for AI-driven threats.

17%

Only 17% of organizations have implemented specific security controls against AI-assisted attacks.

12%

Just 12% have protections in place against deepfake-enhanced voice phishing.

16%

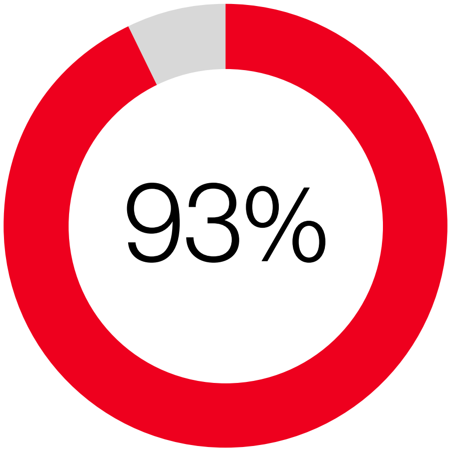
have protections against zero-day exploits.

GenAI adoption outpaces safeguards.

GenAI is a form of artificial intelligence that can create new content, such as text, images, code or audio, based on patterns learned from large datasets. Popular examples include text generators like ChatGPT and image generators like DALL·E, both of which are often used in workplace settings.

Due to the benefits and time savings they offer, genAI tools are being used more widely on mobile devices. That growth also brings new risks.

Despite their concerns, only 45% of organizations provide comprehensive training on the risks associated with mobile AI tools. Half have formal policies in place guiding genAI use on mobile devices. Another 27% say those policies are only loosely enforced.



93% of organizations report employees are using genAI tools on mobile devices.

Figure 2: Widespread genAI use on mobile

93%

of organizations report employees are using genAI tools on mobile devices in their daily workflows.

64%

see data compromise from employees entering sensitive information into genAI as their top mobile device risk.

Human error remains a constant.

Human error refers to mistakes people make that can weaken security, such as clicking on phishing or smishing links, entering sensitive data into unsanctioned apps, or connecting to unsecured Wi-Fi. Despite training and safeguards, these everyday behaviors continue to play a central role in driving mobile risks.

At 44%, user behavior is the top cited breach contributor, just ahead of app threats, network threats and internet threats, which were each cited by 43% of survey respondents. Verizon's 2025 Data Breach Investigations Report found that around 60% of confirmed breaches involved a human element.[2]

Phishing and smishing remain persistent challenges. According to MSI survey data, 80% of organizations reported experiencing mobile phishing attempts targeting their employees. It's not surprising, therefore, that many organizations surveyed (80%) use smishing simulations to help employees gain greater awareness of cybersecurity threats. Among those running simulations, 39% reported that between a quarter and half of their employees clicked a malicious link when tested.

Verizon's 2025 Data Breach Investigations Report found that around 60% of confirmed breaches involved a human element.

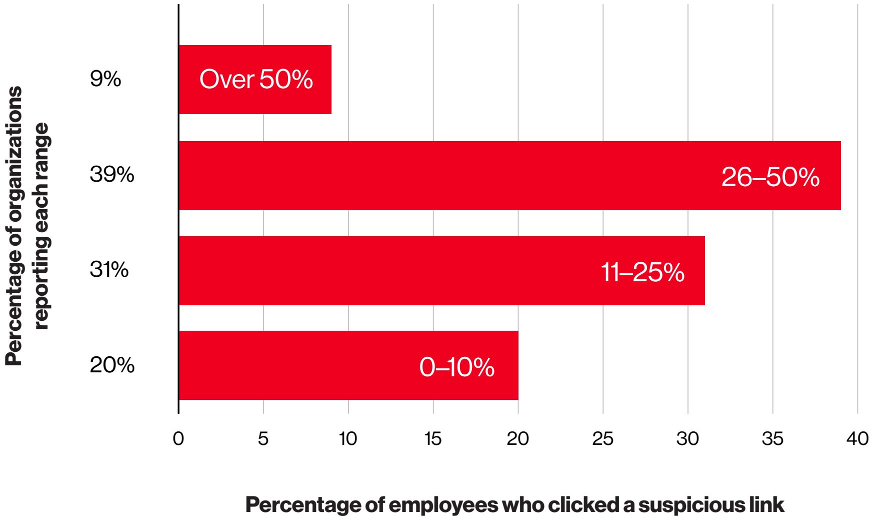


Figure 3: Percentage of employees who clicked on a suspicious link in last smishing test

This year's survey data shows clear implications for organizations: As AI creates new ways for attackers to exploit human behavior and compromise mobile devices, the resulting risks can quickly spread across networks of every size. To respond, proven mobile security approaches are needed to help contain and address these emerging threats.

[2] "2025 Data Breach Investigations Report," Verizon, Apr 21, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Partner insight

Defending against human-centric threats–Lookout Inc.

Human-centric threats drive a new mobile security imperative.

The cyberthreat landscape has fundamentally changed, with attackers now targeting the enterprise's most vulnerable element: humans. As employees work and access cloud data fluidly across personal and corporate mobile devices, attackers are shifting to human-centric threats that exploit behaviors, decisions and social interactions. Their ultimate goal is to obtain login credentials to gain unauthorized access to company resources and sensitive data.

Mobile devices have become the most direct path between attackers and their victims. Always on and deeply personal, these devices offer cybercriminals a rich opportunity to leverage sophisticated social engineering techniques that traditional security tools cannot detect. With AI enhancing the effectiveness of smishing, executive impersonation and multifactor authentication (MFA) token theft, individuals are now even more susceptible to these social engineering techniques.

Today's attacks unfold far beyond email. Threat actors are leveraging SMS, voice and messaging apps to engage in seemingly authentic communications that exploit trust and familiarity. The result is that time to respond has diminished greatly, leaving organizations just minutes to catch and contain the threat before it wreaks havoc on their infrastructure.

To protect against this growing threat, organizations need mobile security strategies that are cloud-native by design, ensuring they can scale to provide real-time visibility into mobile activity.

This approach enables the rapid detection of human-centric threats and the ability to take swift, informed action before an incident spreads. Modern mobile security must do more than protect devices; it must protect people from deception and exploitation and close critical blind spots that happen most naturally at the mobile edge.

To protect against this growing threat, organizations need mobile security strategies that are cloud-native by design, ensuring they can scale to provide real-time visibility into mobile activity.

Firas Azmeh
President

Mobile Endpoint Security, Lookout Inc.

The disruptive impacts of mobile security compromise

The consequences of a mobile security incident can be significant and often lead to downtime.

The reported consequences of mobile breaches can be significant. Organizations reported negative outcomes from a breach, including downtime, data loss, financial penalties, reputational damage and regulatory issues. These reported repercussions underscore some potential impacts that can occur when a mobile device is compromised.

Overconfidence leaves organizations unprepared.

Confidence levels among organizations in detecting and recovering from mobile security breaches remain strikingly high. Of those surveyed, 91% are confident employee misuse of mobile devices would be spotted quickly, with 47% very confident. And 96% say they are somewhat confident or very confident they could recover quickly from a mobile attack; 52% say they are very confident in that belief.

Yet the survey data shows a gap between that confidence and reported consequences.

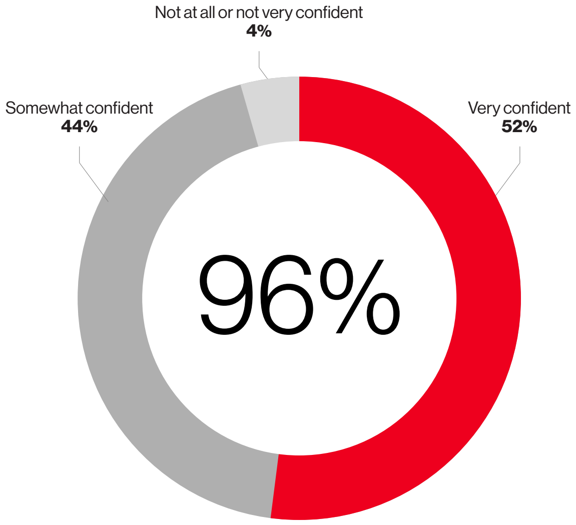


Figure 4: Confidence in quick recovery from a mobile security incident

32%

of organizations that felt very confident they could recover quickly from a compromise still reported major repercussions.

36%

of respondents that suffered downtime from a mobile security incident say remediation was challenging and costly.

The high cost of compromise

The MSI indicates that when incidents do occur, they rarely have a single effect. Among surveyed organizations that experienced a mobile-related security incident, 47% reported downtime, 45% reported data loss, and 40% reported financial penalties or fines.

Another 28% reported reputational damage, while 22% reported that they faced regulatory action – all potentially costly impacts that can quickly spread across the organization.

Downtime disrupts operations.

Compared to the previous year, downtime stands out as one of the most disruptive consequences of a mobile security breach cited by respondents. And the impact appears to be intensifying.

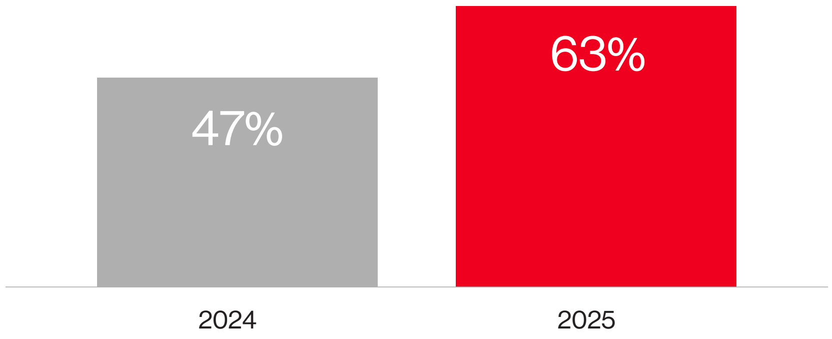


Figure 5: Respondents that experienced major repercussions from downtime after cyberincident 2024–2025

63%

of organizations that suffered downtime reported major repercussions—a 16-point increase over the 47% reported in the 2024 MSI.

Extended business downtime highlights how mobile security incidents can reduce productivity and strain operations in the aftermath of the event.

Risks include data loss and downtime.

Data loss was reported almost as often as downtime (50% compared to 46%). Beyond reported cases, data loss remains the consequence respondents worry about most, cited by 49% of organizations surveyed.

Their concern is well founded.

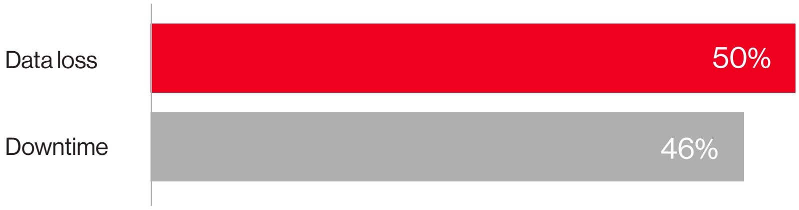


Figure 6: Data loss and downtime reported from mobile security/IoT incidents

Insurance penalties and other real-world outcomes

The consequences of compromise are not limited to technical disruption. Of organizations surveyed, 36% experienced cyber insurance penalties such as higher premiums, reduced coverage or denied claims. In fact, this insurance impact was cited by respondents more often than any other real-world consequence.

Additionally, 60% of organizations report that they carry cyber insurance, suggesting that while many organizations seek to transfer some risk, possible gaps in policy coverage leave open the potential for costly remediation.

The broader ripple effect

Taken together, the survey results show that mobile security incidents can lead to downtime, data loss, financial penalties, reputational damage and regulatory issues. These outcomes highlight the downstream consequences of compromise that can extend well beyond the device and potentially have more severe effects on daily operations and business continuity.

50%

of organizations had a mobile or Internet of Things (IoT) security incident that resulted in data loss.

46%

of organizations had a mobile or IoT security incident that resulted in downtime.

Rising investments, stronger defenses

To defend themselves, most organizations are ramping up spending on mobile security, employee training and smarter tools.

Given rising threats to mobile devices, organizations are shoring up security with tangible investments. Budgets for mobile security are expanding; mobile security training programs are reaching more employees; and many are shifting to company-owned devices to improve control.

The goals for these investments go beyond preventing incidents to include risk reduction, efficiency and productivity. This highlights how mobile security today is viewed as both a safeguard and an enabler of day-to-day operations.

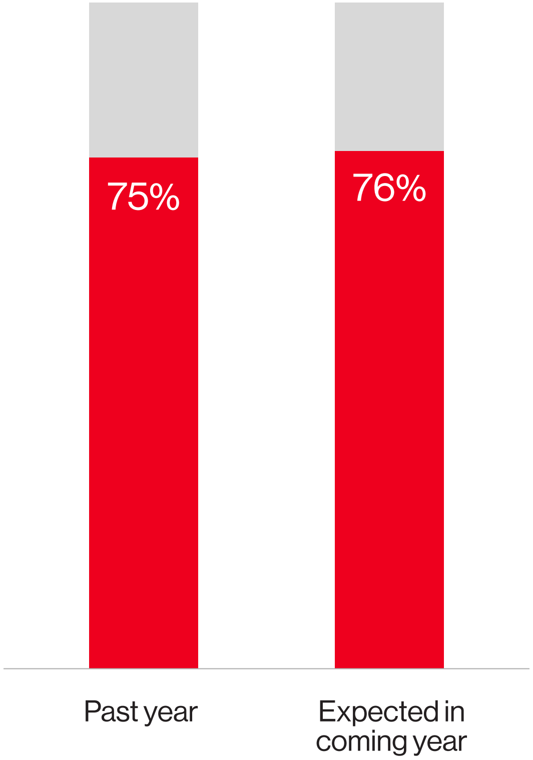


Figure 7: Organizations with increased mobile security spending

75%

of organizations have increased mobile security spending in the past year.

76%

believe their mobile security budgets should increase again in the coming year.

Mobile security investment is on the rise.

Survey results reflect a growing recognition that mobile security is increasingly on the radar of organizational leadership, influenced by a growing understanding of today's mobile security risks, compliance requirements, and by the practical realities of a mobile and distributed workforce.

For example, most organizations have formal security budgets in place, with 80% of organizations we surveyed reporting a defined overall security budget. Of those with a defined security budget, a robust 89% have a specific amount earmarked for mobile security. What's more, 75% of organizations surveyed increased mobile security spending in the past year. And 76% of organizations polled believe their mobile security budgets will increase again in the coming year.

When asked what's driving these investments, respondents cited greater threat awareness (48%), more users (43%), increasing threats (42%), more devices (41%), compliance (41%), more apps (41%), and a remote or hybrid workforce (39%).

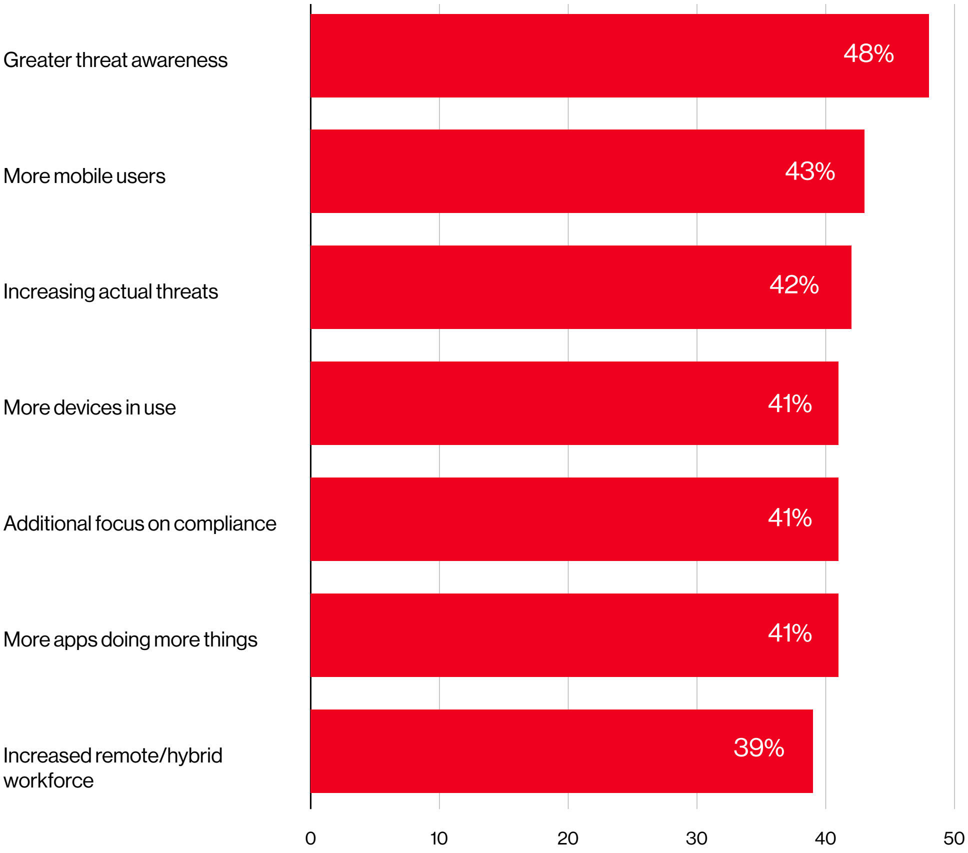


Figure 8: Drivers behind increased mobile security spending

When asked what's driving these investments, respondents cited greater threat awareness, more users, increasing threats, more devices, compliance, more apps, and a remote or hybrid workforce.

84%

The biggest influence, however, may be the cost of doing business today. Of organizations surveyed, 84% reported that a client, partner, regulator or insurance provider demanded they demonstrate the maturity of their mobile device security strategy. That need, along with the growing list of threats facing security teams, may be enough to make the case to the C-suite, board members and shareholders that organizations can't afford to ignore potential cyber risks.

Employee training is expanding, but there's still room for improvement.

The majority of organizations are also making investments in employee mobile security awareness through phishing and smishing training and simulation testing.

For example, 62% of organizations surveyed provide mobile security training when onboarding new employees and 58% do so when issuing new devices. However, there's still room for improvement among organizations that don't provide this training.

A more encouraging development – especially in the face of more sophisticated, AI-powered mobile device hacking attempts – is that more organizations are taking AI risk training seriously.

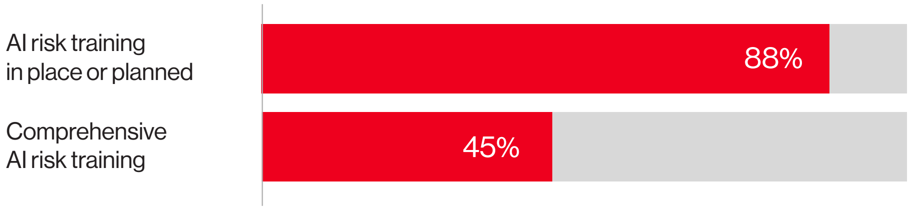


Figure 9: Organizations performing AI risk training

88%

have or are planning AI risk training.

45%

describe that training as comprehensive.

76%

of organizations reported they run phishing or smishing drills at least annually.

Concession devices are favored by a majority.

Company-provided mobile devices, also known as concession devices, are one way organizations can help reduce risks that are often associated with bring your own device (BYOD) environments that allow employees to use their personal mobile devices for work.

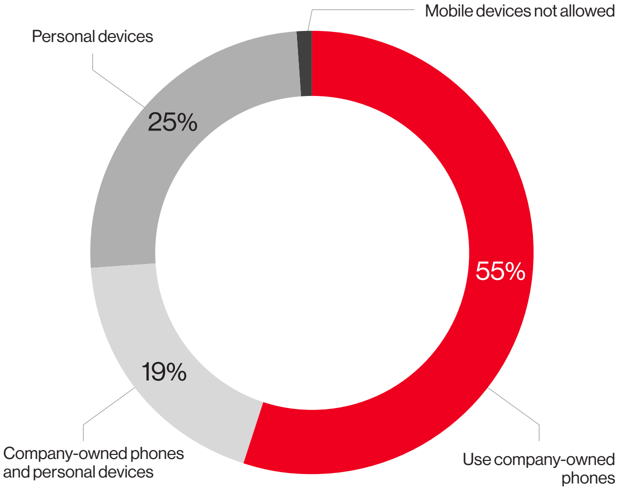


Figure 10: Use of company-owned phones vs. personal devices

55%

of organizations say they provide company-owned or concession devices.

19%

use a mix of concession and personal devices.

74%

offer some form of company-provided mobile device support.

25%

allow their employees to use personal devices.

1%

do not allow mobile devices for work purposes.

Best practices adoption shows results.

The survey included eight mobile security best practices and asked respondents to indicate which ones they have implemented.

Even though only 4% of organizations surveyed reported that they have implemented all eight best practices, the results of doing so are impressive. Those that did were half as likely to report experiencing downtime from a mobile-related incident and five times less likely to report major repercussions.

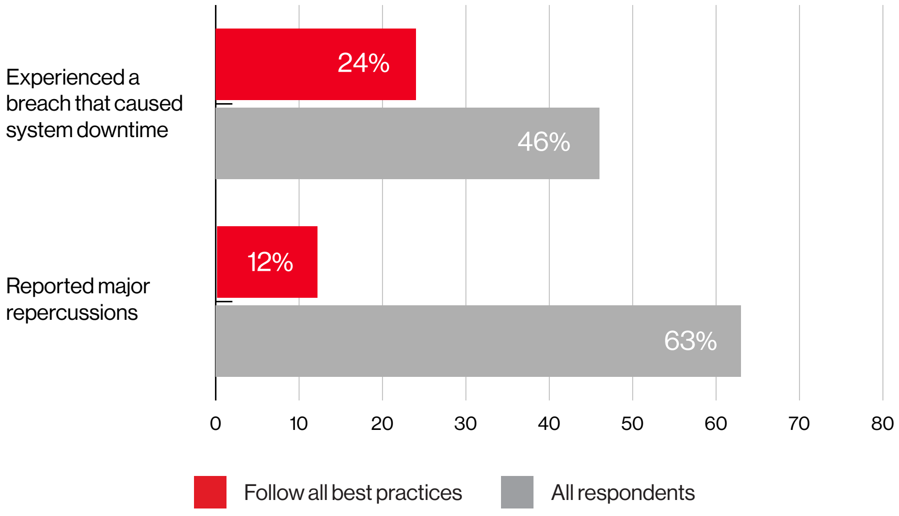


Figure 11: Outcomes when all mobile security best practices are used

Within the 4% group, 24% experienced a breach that caused system downtime, compared with 46% of all respondents that experienced downtime when the organization did not implement all eight security best practices. What's more, of the organizations that implemented all eight best practices, just 12% reported major repercussions, compared with the overall survey average of 63%.

Analyzing this group shows that comprehensive adoption of security best practices can pay dividends, but it also highlights how much progress remains for the majority of organizations.

Eight trusted mobile cybersecurity best practices

- **Mobile device management (MDM) and unified endpoint management (UEM):** Using a single platform to centrally manage, secure and update all user devices, including laptops, phones and tablets
- **Mobile threat defense (MTD):** Detecting and blocking mobile-specific risks such as phishing, malicious apps and device compromise in real time
- **Zero trust:** Verifying every user and device before granting access to the network – regardless of location – to reduce insider and credential-based threats
- **Secure access service edge (SASE):** Combining network and security services such as firewalls and secure web gateways to protect remote and hybrid workers through the cloud
- **Secure enterprise browser and secure web gateway:** Enforcing security controls within the browser to protect access to cloud and web apps; ideal for zero trust and remote work environments
- **Endpoint detection and response (EDR):** Monitoring mobile and endpoint activity to detect, investigate and automatically respond to threats across devices
- **Managed detection and response (MDR):** 24/7 expert threat detection and incident response as a managed service, often powered by EDR tools and threat intelligence
- **Cyber risk quantification (CRQ):** Translating cyberthreats into financial impact to guide investments, board conversations and cyber insurance decisions

A mix of security tools and policies are in use.

Organizations report mixed adoption of foundational access controls and policies that they use to help enhance mobile security.

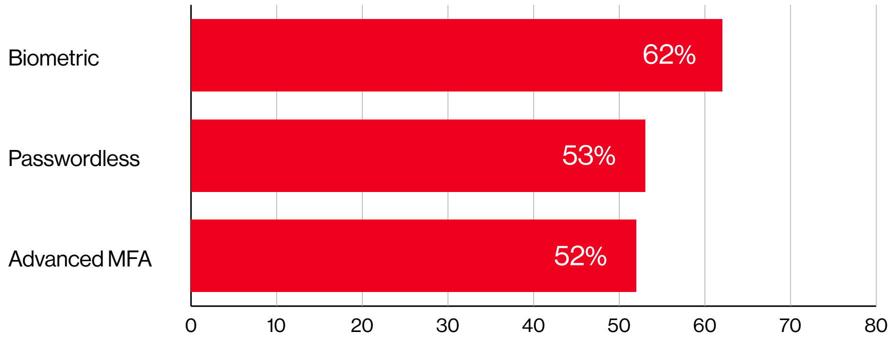


Figure 12: Adoption of mobile access controls

Identity protections are also advancing. Of organizations surveyed, 62% use biometric authentication. And 53% of respondents report using passwordless or passkey access. In addition, 52% of respondents said they use advanced MFA.

Separately, another 62% report using AI-powered software to automatically revoke mobile access privileges based on risk signals.

Enhanced security and operational efficiency are top objectives.

The survey indicated clear objectives driving organizational investment and technology decisions. While enhancing mobile security tops the list of objectives, operational efficiency objectives are not far behind.

The organizations surveyed said they are investing to:

- Enhance security for current user activities (51%)
- Reduce the risk of breaches or incidents (49%)
- Reduce IT workload (42%)
- Improve user experience and productivity (42%)
- Enable secure access to new services for remote workers (41%)
- Unify security management across mobile devices (34%)

Taken together, these objectives and the increased spend noted by most organizations surveyed show progress in terms of bigger budgets, broader employee training and smarter tools. This indicates there's more buy-in on the benefits of expanded mobile security from organizational leadership.

Yet remaining gaps leave openings that adversaries may exploit. Achieving mobile security resilience will depend on not just spending more but also on applying investments effectively across both the workforce and the organization's mobile device infrastructure. This is true especially in the face of AI-powered threats and ongoing human error.

60%

use role-based access control.

52%

have an incident response plan.

50%

enforce an acceptable use policy.

9%

acknowledge having no formal access controls.

Partner insight

Securing the hyperconnected mobile enterprise with hybrid mesh architecture–Check Point Software Technologies Ltd.

The risks

Organizations are navigating a challenging hyperconnected, AI-powered world where innovation is rapid, but so are the threats. As advanced mobile threats become more prevalent, organizations need to understand that mobile and IoT devices used for critical business communication have become significant targets for cybercriminals. With the growing reliance on wireless communication and remote work by both businesses and government agencies, attackers are leveraging spyware, phishing schemes, social engineering, zero-click exploits and new AI-enhanced threats to access sensitive information, impact businesses and introduce risk to critical infrastructure. Applications used for email, collaboration and file-sharing have also become vectors for account takeover and business email compromise, data loss, harmful malware, and expensive ransomware events.

The solution

To increase the efficacy of security programs in response to these new mobile threats, organizations should take a proactive stance by implementing a comprehensive security architecture that goes beyond just zero-trust network access (ZTNA). AI-based threat prevention that includes protection for mobile devices and for critical business communication applications such as email, collaboration and file-sharing applications is paramount. Achieving successful security outcomes requires a comprehensive approach with a collaborative framework for intelligence sharing and tight integration between security tools.

Beyond ZTNA: Hybrid mesh security architecture

The hybrid mesh security architecture is a modern, diverse and decentralized security and networking architecture where cloud-based security controls and policy enforcement are embedded directly into distributed network nodes across network edge, IoT/operational technology (OT), mobile devices, branches, clouds, data centers and applications. When deployed, it enables fast, scalable, automated and adaptive protection by pushing intelligence and enforcement to the interconnected nodes.

Secure, efficient and effective business communication needs to be multifaceted and include threat prevention for mobile devices as well as interconnected business applications. Organizations that seek strong security outcomes should adopt a prevention-first hybrid mesh security architecture as part of their enterprise security strategy to better safeguard their digital resources.

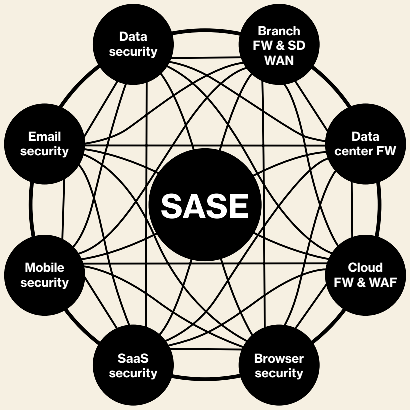


Figure 13: Hybrid mesh architecture for network security

Peter Nicoletti
Global CISO

Check Point Software Technologies Ltd.

Managing devices, managing risk

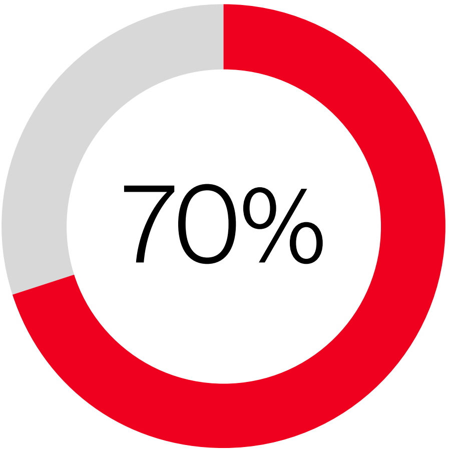
Organizations using MDM tend to have stronger security policies, especially for AI.

MDM is helping organizations build stronger, more consistent defenses. Organizations using MDM report more comprehensive training, clearer policies and stronger enforcement – especially for AI-related risks.

In contrast, organizations that have considered but rejected MDM faced higher rates of lost data. Of organizations that rejected MDM, 63% experienced lost data, compared with 50% overall. Among this group, 31% also described their risk as extreme, more than double the 15% study average.

Personal devices are shown to increase attack exposure.

Based on survey responses, the added risks of using personal devices for work are noteworthy: 70% of mobile devices impacted by an attack are personal, not corporate-issued.



70% of mobile devices impacted by an attack are personal rather than corporate-issued.

Figure 14: Personal devices drive higher risk.

What's more, the limits of control in environments that use personal (BYOD) and/or unmanaged devices mean that visibility may be impacted and mobile security remains a challenge. In total, 45% of organizations surveyed report that it's difficult to detect shadow IT activity due to missing or incomplete data, and 41% say it's challenging to identify specific vulnerabilities.

The diversity and volume of device types also continue to expand organizational attack surfaces. For example, 51% of organizations surveyed expect the number of IoT devices they manage to increase in 2025. This could potentially impact operational technology (OT) environments that heavily leverage IoT in critical infrastructure industries such as energy, manufacturing and transportation.

When organizations allow only company-owned devices and already use MDM, the rate of defined and enforced genAI usage policies rises to 66%.

What is MDM?

Mobile device management (MDM) enables businesses—from a small business with no IT staff to a large enterprise—to manage a wide range of devices that access company apps and resources.

MDM solutions help manage devices, employee access, privileges and policies. These solutions also help businesses control vulnerabilities in their software and hardware.

MDM can strengthen AI threat readiness.

Device management decisions were correlated with mobile security defenses and outcomes. For example, several mobile security advantages were reported by those using MDM, including consistently stronger protections and fewer negative outcomes, compared to organizations not using MDM.

- In particular, 55% of MDM users surveyed provide comprehensive AI risk training, compared to only 39% of organizations that do not use MDM – a 16 percentage-point improvement.
- Additionally, 59% of MDM users surveyed have defined and enforced genAI usage policies; that percentage drops to 45% among respondents that do not use MDM.
- 63% of MDM users surveyed regularly audit AI-generated content, while only 48% of organizations without MDM report doing so.
- 71% of MDM users surveyed automatically revoke mobile access privileges based on risk signals, compared with 57% of respondents that do not use MDM.

These survey responses show how MDM not only serves as a foundation for improving mobile security and governance, but MDM also is associated with the added value of enhancing policy enforcement in ways that directly address AI-related risks.

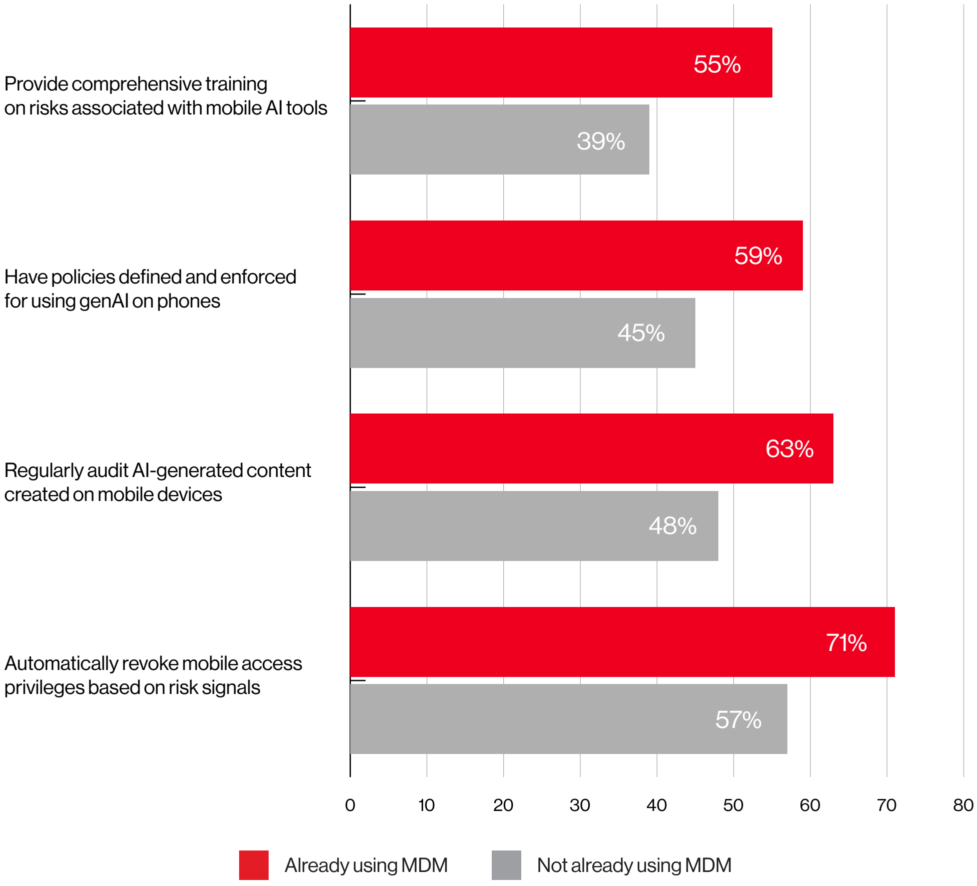


Figure 15: MDM use is associated with stronger AI threat defenses.

Rejecting MDM can leave organizations vulnerable.

The gap in mobile security incident outcomes widened significantly among organizations that considered but rejected MDM.

Of organizations that rejected MDM, 63% experienced lost data, compared to 50% for all respondents.

Among the group that rejected MDM, 31% also described their risk of mobile device threats as extreme – more than double the 15% study average.

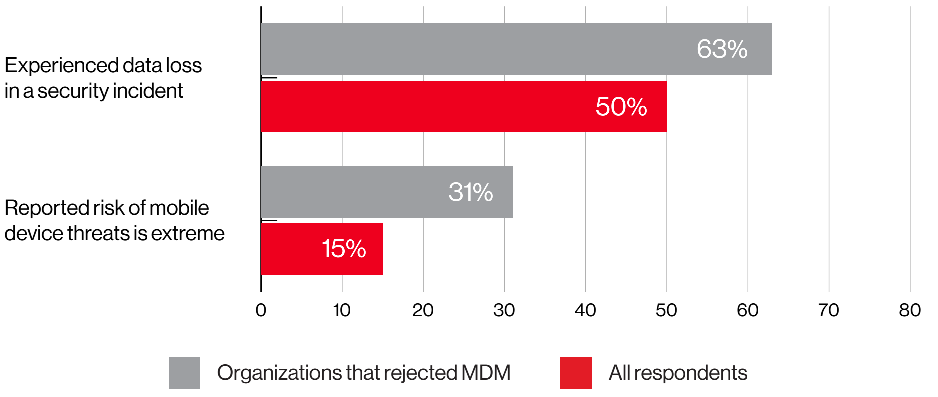


Figure 16: Negative outcomes reported by organizations that rejected MDM

Declining to adopt MDM not only limits visibility and control over mobile devices, but lack of MDM also correlates with both higher perceived risk and greater incidence of data loss.

Declining to adopt MDM not only limits visibility and control over mobile devices, but lack of MDM also correlates with both higher perceived risk and greater incidence of data loss. The contrast between respondents using MDM and those rejecting it is clear: MDM users report stronger policies, better enforcement and fewer incidents.

Partner insight

Why MDM is essential for securing BYOD environments– Ivanti Inc.

Security concerns are rising as more employees work both in and out of the office, and BYOD is today's workplace reality. Recent data shows that three in four IT workers say BYOD is a regular occurrence, but only 52% report that their organizations explicitly permit it. Even more concerning, among the organizations that formally prohibit BYOD, only 22% say employees actually comply.

BYOD risk mitigation maneuvers

A clear and enforceable BYOD approach is essential. BYOD policies should directly address the real-world risks posed by personal devices in the workplace. For example:

- **Eligibility:** Clearly define which employees are authorized to use personal devices for work. Specify allowed device types and outline necessary security measures, such as encryption and strong password management.
- **Responsibility and compliance:** Implement policies requiring users to accept MDM protocols, enabling the organization to remotely wipe devices if security is compromised.
- **Data management and privacy:** Establish and document the level of access permitted for BYOD devices. Avoid granting unmanaged devices full network access. Instead, use a least-privileged access model and set clear guidelines on which data and applications can be accessed.
- **Support and maintenance:** Maintain an up-to-date inventory of approved devices. Devices with unsupported operating systems or outdated apps can increase support costs and hinder productivity.
- **Exit planning:** Develop comprehensive procedures for removing access and corporate data from personal devices when an employee leaves or loses BYOD privileges, ensuring all connections to the organization's network are fully severed.

As security concerns continue to rise, 29% of security professionals cite BYOD itself as a heightened risk, closely followed by the use of unapproved software (28%) and employees permitting friends or family members to use work devices (27%).

Using MDM to address BYOD dilemmas

Alongside policies and training, organizations need a robust MDM solution capable of overseeing every personal device used for work. Effective platforms should include features such as device enrollment, application oversight, remote wiping and compliance enforcement. Addressing these challenges head-on will help organizations to harness the productivity benefits of BYOD while minimizing risk.

Karl Triebes
Chief Product Officer

Ivanti Inc.

Understanding SMB and enterprise challenges

SMBs feel targeted but underprepared.

Small- and medium-sized businesses (SMBs) find themselves in a difficult position. Security leaders in this segment say their organizations are more of a target for cyberattackers than larger enterprises, yet they tend to invest less than enterprises in the mobile security policies and defenses that could reduce their risk.

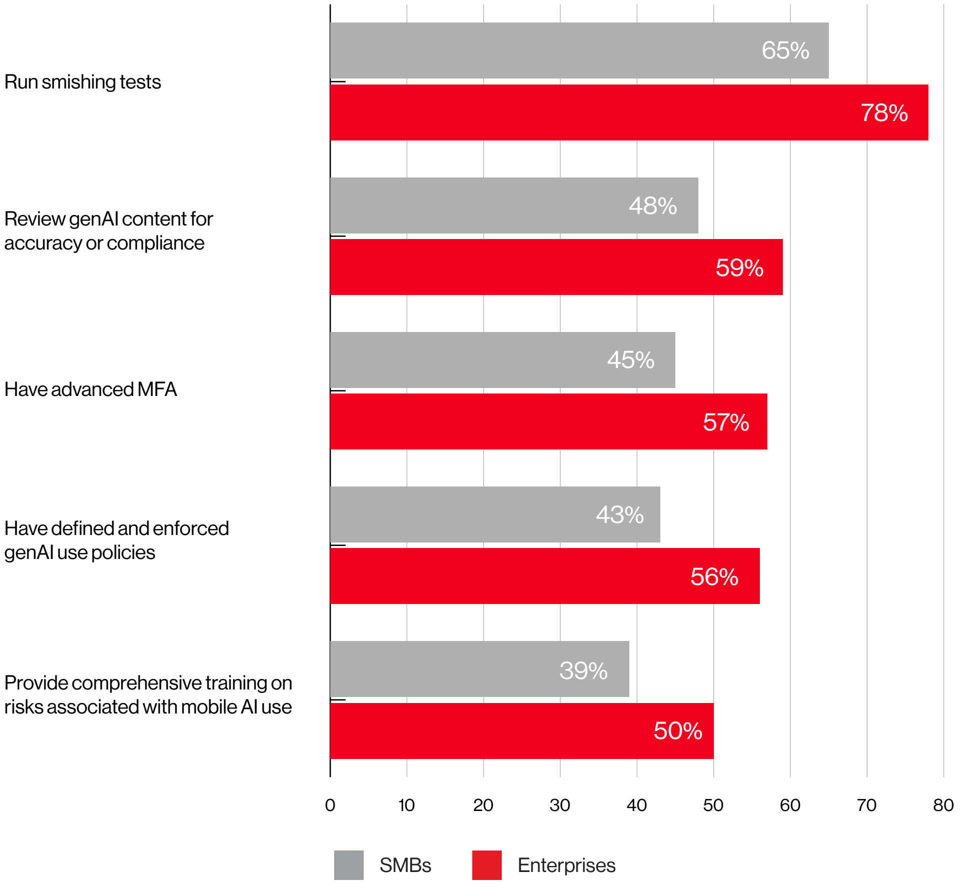


Figure 17: SMBs report lower adoption of mobile security measures vs. enterprises.

57%

of SMBs agree that they are at a disadvantage in terms of resources, making it harder to respond to cybersecurity attacks than larger enterprises—and 61% of enterprise respondents agree.

54%

of SMBs—and 55% of enterprises—also say SMBs have more to lose from a security breach.

Yet SMBs reported being less likely than enterprise businesses to take proactive steps to protect against mobile security threats. Failure to define and enforce policies, train employees or deploy key cybersecurity defenses can increase the risk of an attack, which can disrupt business operations or lead to a potential hit to the bottom line.

SMBs surveyed fall behind enterprises in adopting proactive mobile security measures. These include testing, policy enforcement, authentication practices and training programs.

These gaps show how SMBs often remain more exposed, even when they recognize the risks. The contrast becomes clearer when looking at how enterprises approach mobile security.

Enterprises adopt more controls yet face greater impact.

Enterprises face different challenges than SMBs. Survey results show that enterprises are more proactive in defenses and training than SMBs, but they face a higher percentage of attacks.

- Enterprises generally outpace SMBs in their adoption of common cybersecurity defenses such as MDM (43% of enterprises adopting defenses vs. 33% of SMBs surveyed), CRQ (48% vs. 38%) and zero trust (47% vs. 38%).
- Enterprises are more likely than SMBs to change default passwords daily (16% of enterprises changing default passwords daily vs. 10% for SMBs surveyed).
- Enterprises are also more likely to train employees on mobile security when they first join (66% of enterprises vs. 56% of SMBs) and provide such training on a quarterly basis (51% for enterprises vs. 40% of SMBs surveyed).

Even with their greater adoption of controls, 52% of enterprises surveyed experienced a mobile cyberattack that resulted in system downtime, compared to 37% of SMBs. This higher attack rate may be attributed to multiple factors within enterprise organizations, such as:

- Larger employee populations and more mobile devices that increase opportunities for mistakes or misuse
- Better incident detection and reporting within enterprise environments
- Overly complex software approval processes that increase the risk of employees circumventing controls

Enterprises generally outpace SMBs in their adoption of common cybersecurity defenses such as MDM (43% of enterprises adopting defenses vs. 33% of SMBs surveyed), CRQ (48% vs. 38%) and zero trust (47% vs. 38%).

And human error is a factor, as 47% of enterprise respondents say user behavior, such as falling for phishing or smishing or installing unauthorized apps, contributed to a compromise – compared with 39% of SMBs saying user behavior is a factor.

Better training and policy enforcement could help, especially for employees tasked with managing sensitive corporate or customer data. Taking steps to prevent errors, such as resolving database misconfigurations that are common among enterprises, may also help.

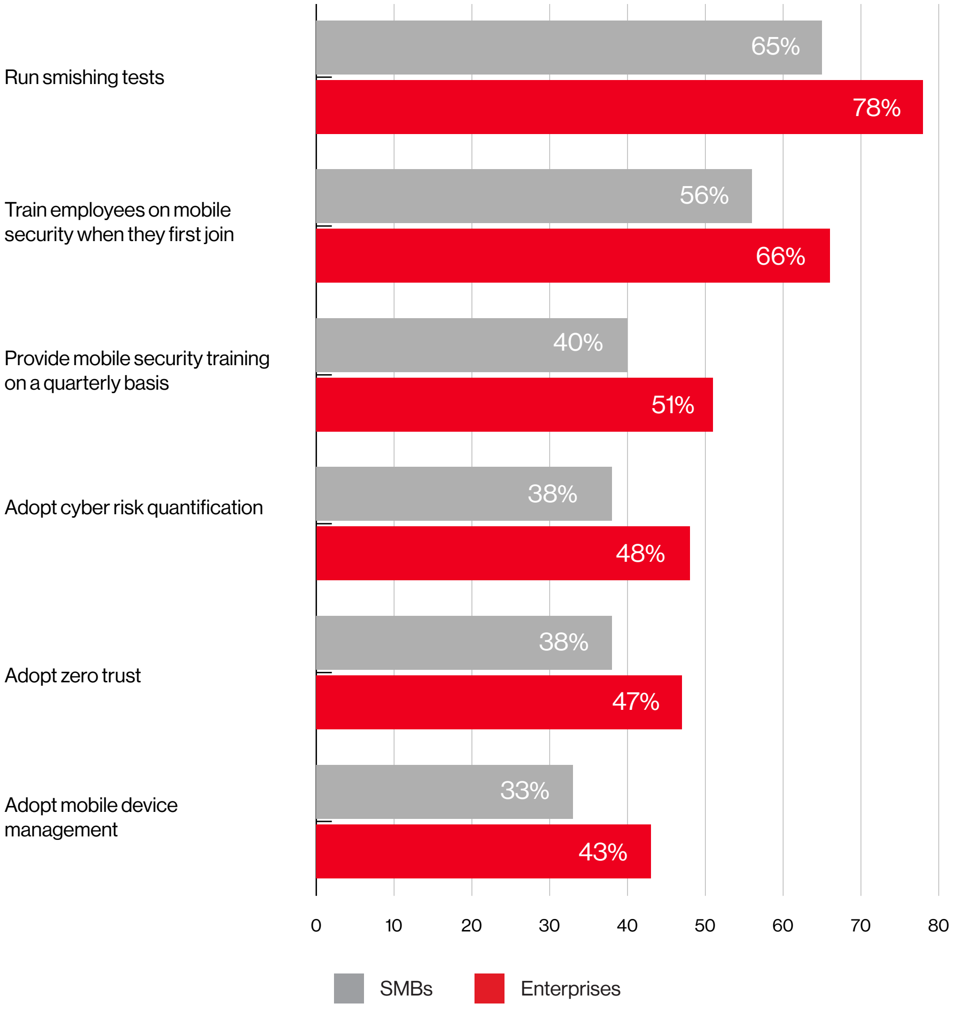


Figure 18: Mobile security practices, enterprises vs. SMBs

User behavior remains a shared weakness.

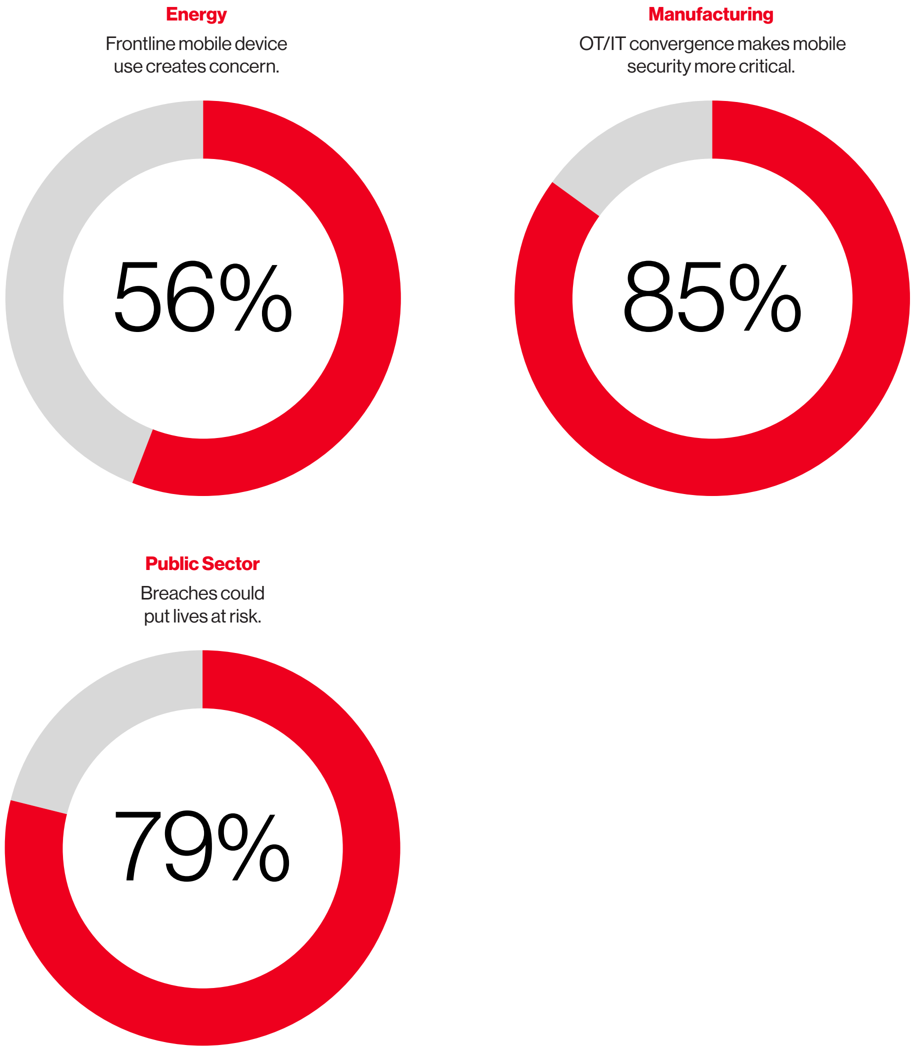
Despite the differences between SMBs and enterprises, threats that rely on human error are a shared concern. Enterprises that train their employees against phishing and smishing attacks do so with virtually the same frequency (46%) as compared to SMBs (45%).

Industry and segment spotlights

Mobile security concerns persist in energy and manufacturing, and the Public Sector is working to address public expectations.

Respondents were grouped into several industries or segments. Not surprisingly, each sector reported some unique challenges when it comes to mobile device security.

In particular, energy, manufacturing and Public Sector organizations reported heightened risks from mobile and IoT threats, making these sectors stand out for the unique security challenges they face.



Energy

Frontline mobile device use creates concern.

Manufacturing

OT/IT convergence makes mobile security more critical.

Public Sector

Breaches could put lives at risk.

Figure 19: Mobile risk factors vary by industry.

90%

of retail organizations rated the cybersecurity awareness of their shop floor employees, frontline workers and field workers as high or medium.

89%

of healthcare organizations are concerned or very concerned that a security breach could seriously compromise patient care.

86%

of financial services organizations said cybercriminals see their companies as more lucrative targets than other industries.

Energy:
Increased exposure, uneven preparedness

Security leaders in the energy industry believe they're an attractive target for cyberattacks, given their role in supporting critical infrastructure and their increased use of mobile devices for field workers.

Respondents in this sector have taken some steps to improve their security posture. They've almost universally updated mobile security controls, for example. But they also report they're lagging in the adoption of key mobile security and incident response best practices compared to other sectors.

- 72% of energy organizations say they're a prime target for cybercriminals given their critical infrastructure role.
- According to Lookout, 23.7% of employees at energy and utility companies were targeted by mobile phishing in the first quarter of 2025.[3]
- 100% of energy industry survey respondents say they have taken action to update mobile security controls for AI-assisted attacks and zero-day exploits; 97% have done so for deepfakes.

Energy sector respondents report lower adoption of several cybersecurity defenses compared to all industries.

For example:

- Only 39% of energy respondents use SASE, compared to 49% across all industry respondents.
- 34% use enterprise browsers, compared to 45% across all industries.
- 35% have implemented zero trust, compared to 43% across all industries.
- 35% use MDM, compared to 38% across all industries.

Energy respondents also lag in key preparedness measures. Just 35% have a disaster recovery plan they can quickly act on, compared to 42% of respondents from other industries. Only 34% maintain a ransomware playbook (vs. 39% of respondents from other industries), and 52% carry cyber insurance, compared to 60% of respondents from other industries.

The picture that emerges is of a sector making progress but still carrying significant exposure, as adversaries target critical infrastructure.

100%

of energy respondents say that they have taken action to update security controls to protect against AI-assisted and zero-day attacks.

But energy sector respondents report lower adoption of several cybersecurity defenses compared to all industries.

[3] "Lookout Mobile Threat Landscape Report - Q1 2025," Lookout, 2025. https://www.lookout.com/threat-intelligence/report/2025-q1-mobile-threat-landscape-report

Manufacturing: Supply chain risk and IoT back doors

Similar to energy firms, respondents that identified as part of the manufacturing industry believe their increased mobile adoption, which includes IoT and OT devices, heightens their risk of a cyberattack. Manufacturers further say their interconnected supply chains, which are vital to supporting operations in a competitive global industry, make them more vulnerable to breaches and disruptions. Of those manufacturers surveyed, 83% say a security incident could disrupt their supply chain and have serious reputation implications.

Currently, every unsecured IoT or OT device can serve as a back door into the corporate network, exposing organizations to the potential for operational downtime, data theft and reputational damage. This expanded connectivity helps explain why 85% of manufacturers say convergence of OT and IT makes mobile device security more critical.

Despite their heightened awareness of potential cyber risks, the manufacturing industry is behind other sectors in updating mobile security controls, implementing incident response best practices and closing security gaps associated with genAI use. According to Lookout Threat Labs, 18.5% of employees at manufacturers were targeted by mobile phishing in Q1 of 2025.[4]

Manufacturing trails other vertical sectors in updating mobile security controls for the following types of threats:

- AI-assisted attacks (91% of manufacturing businesses that update AI controls vs. 96% that do in all industries)
- Zero-day exploits (91% of manufacturers that update controls to address zero-day exploits vs. 95% in all other industries)
- Deepfakes (87% of manufacturers that update security to address deepfakes vs. 94% that do in all other industries)

Manufacturing also lags behind most other vertical industries in:

- Defined and enforced genAI policies (37% of manufacturers surveyed vs. 50% in other industries)
- Audits (40% of manufacturers surveyed vs. 54% in other industries
- Comprehensive training on mobile AI tools (39% of manufacturers surveyed vs. 45% in other industries)

In addition, manufacturers are less likely than most other vertical industries to have:

- An acceptable use policy (AUP) (42% of manufacturing companies surveyed said they had an AUP vs. 50% for all industries)
- A disaster recovery plan (36% for manufacturing companies vs. 42% for all industries)
- A ransomware playbook (36% for manufacturing companies vs. 39% for all industries)
- Cybersecurity insurance (57% for manufacturing companies vs. 60% for all industries)

While manufacturers are more likely to use MTD (58% of manufacturing companies surveyed said they use MTD vs. 48% across all industries), they are less likely to use the following mobile technologies:

- Zero trust (35% of manufacturers said they use zero trust vs. 43% across all industries)
- SASE (31% of manufacturing companies said they use SASE vs. 49% across all industries)
- MDR (39% vs. 44%)
- EDR (43% vs. 48%)

85% of manufacturer respondents say convergence of OT and IT makes mobile device security more critical.

[4] "Lookout Mobile Threat Landscape Report - Q1 2025," Lookout, 2025. https://www.lookout.com/threat-intelligence/report/2025-q1-mobile-threat-landscape-report

Public Sector: High stakes and public expectations

Public Sector organizations are under constant pressure to deliver uninterrupted services while protecting sensitive data and infrastructure. That visibility, and the potential consequences of disruption, have led many agencies to adopt more mature mobile security practices.

- 79% of Public Sector organizations say a security breach could put people's lives at risk.
- 84% of Public Sector organizations say the public's expectations for self-service require additional mobile cybersecurity defenses.

This year's report data shows the Public Sector generally leads other sectors and industries in several areas, particularly in addressing genAI-related risks.

Public Sector respondents were slightly ahead of other verticals in updating mobile security controls for the following types of threats.

- AI-assisted attacks (98% of Public Sector organizations vs. 96% for other industries)
- Zero-day exploits (97% of Public Sector organizations vs. 95% for other industries)
- Deepfakes (97% of Public Sector organizations vs. 94% for other industries)

A greater number of Public Sector organizations also reported having policies, audits and training in place to restrict genAI tool use and ensure the accuracy of AI-generated content.

- Defined and enforced genAI policies (58% of Public Sector organizations vs. 50% for other industries)
- Audits (96% of Public Sector organizations vs. 91% for other industries)
- Comprehensive training on mobile AI tools (52% for Public Sector organizations vs. 45% for other industries)

Public Sector organizations also lead other verticals in their use of some mobile security technologies, including:

- SASE (52% of Public Sector organizations surveyed vs. 49% for other industries)
- Enterprise browser (48% of Public Sector organizations vs. 45% for other industries)
- EDR (51% of Public Sector organizations vs. 48% for other industries)

However, Public Sector organizations slightly trail other verticals in their use of other mobile security technologies, such as MTD (42% of Public Sector organizations vs. 48% for other industries) and CRQ (40% of Public Sector organizations vs. 43% for other industries).

These findings underscore how visibility and accountability remain central to mobile security efforts in the Public Sector.

79%

of Public Sector organizations say a security breach could put people's lives at risk.

Public Sector organizations are under constant pressure to deliver uninterrupted services while protecting sensitive data and infrastructure.

It’s time to act

Business owners face multiple cybersecurity pressures, including quickly evolving AI-driven threats, persistent human error, and rising expectations from management, customers and regulators. This year’s report shows that while awareness of and investment in mobile security are increasing, too many organizations still have mobile security gaps, including uneven policy enforcement, risky BYOD approaches and too few best practices applied.

To reduce exposure and improve resilience, take these recommended steps to help enhance your mobile security posture.

1. Start with the basics.

Build or revisit your written AUP (be sure to include AI guidelines). Once you have a guiding document, implement an MDM solution across all managed and BYOD devices. MDM helps you set policies and control mobile device configurations, usage and security. Organizations using MDM report having stronger mobile security protections and fewer negative outcomes, underscoring MDM’s value as a critical basic safeguard for mobile environments. MDM also:

- Helps with patch management to ensure that mobile endpoints are updated with the latest patches to help protect against vulnerabilities as they are discovered.
- Helps control which apps users can install on their mobile devices and prohibit apps that are not from an official or company store from being installed on devices to help avoid malware-infected apps.
- Helps align genAI use with defined, enforced policies and role-based access controls. Establishing clear guardrails helps AI-driven innovation to advance business goals while limiting risks related to misuse, data leakage or unauthorized access.

It's time to act

2. Evaluate your mobile cybersecurity protections using industry standards and best practices to identify any gaps.

Adoption of the following eight mobile security best practices can significantly lessen the risk of cyberincidents and repercussions. Following a multilayered set of cybersecurity defenses can help reduce vulnerabilities across devices, networks and applications while strengthening resilience against evolving threats. The best practices identified in the report highlight these layers of defense.

- MDM solutions help to centrally manage, secure and update mobile devices.
- MTD solutions offer antivirus and antimalware protection, as well as phishing protections, to help protect against credential theft.
- Zero-trust solutions provide continuous user access verification to critical data and applications to help reduce credential-based threats.
- SASE solutions that combine cloud-based network and security services such as firewalls and secure web gateways help protect remote and hybrid workers.
- Secure web gateway solutions help enforce internet security controls within the browser to protect access to cloud apps and web content.
- Endpoint detection and response solutions monitor mobile and endpoint activity to help detect and automatically respond to threats across devices.
- Managed detection and response services provide 24/7 expert threat detection and incident response as a managed service.
- Understanding and quantifying your cyber risks and risk tolerance helps identify and prioritize security investments to meet key business and security objectives.

3. Enhance your mobile security while improving operational efficiency.

Investment in zero-touch mobile security solutions can not only reduce risk but can also help reduce IT workload, with many organizations citing this as a key investment objective.

- When adopting a multilayered approach to security, consider the speed and complexity of deployment and simplicity of operational burden.
- Zero-touch mobile security solutions built into mobile networks offer additional protections without the need for installation or management of software or apps on mobile devices. This can greatly benefit organizations where IT or security resources are limited, making it easier to scale protections without adding staff or operational overhead.
- Solutions that help automate mobile threat detection and credential protection where possible help reduce the burden on security teams by enabling automatic updates and scans.

It's time to act

4. Fight the threat of phishing by implementing continuous, adaptive training and testing.

Given the persistency of human error related to smishing and phishing attacks, all organizations should be investing in threat training and testing to help employees better identify and report those types of threats.

- Teach employees how to recognize and report phishing, whether it comes via email, calls, apps or SMS.
- Require mandatory retraining for those who score poorly.
- Conduct regular simulation testing with practical exercises that help employees recognize and resist the latest social engineering tactics, which can subsequently help reduce the risk of human error.
- Configure your mail system to flag emails from outside your domain. For example, many companies add a prefix, such as [E], to the subject line that can help employees spot potential phishing emails.

Together, these steps help create the guardrails organizations need to navigate the perfect storm of AI-driven threats and human error in today's mobile world. They can help strengthen not only mobile security but also business continuity, regulatory readiness and stakeholder confidence. The organizations best positioned to lead are not those that say they are prepared to address cyberthreats but those that can demonstrate it.

Appendices

Survey methodology

In April 2025, Verizon commissioned an independent market research company to survey SMBs, enterprise organizations and Public Sector entities. Participants included employees and staff involved in the procurement, management and security of mobile devices. In total, 762 professionals took part.

The charts below break down respondent and organizational demographics, spanning small organizations through large enterprises. Respondents were distributed across seven vertical sectors, three regions, three organization size categories and seven functional roles.

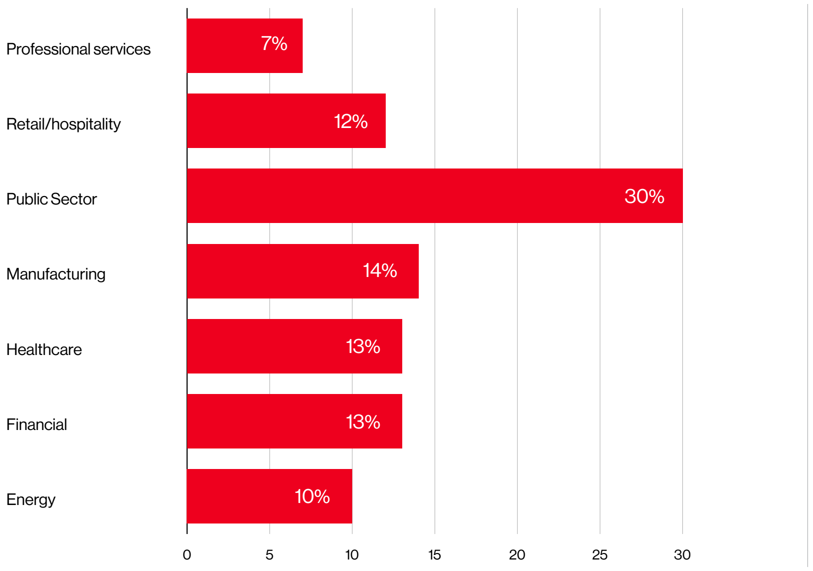


Figure 20: Industry sectors represented

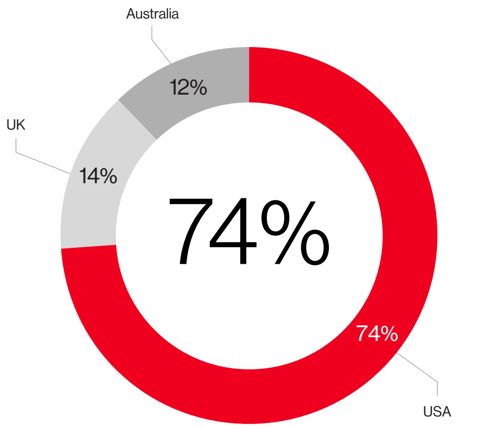


Figure 21: Regional location

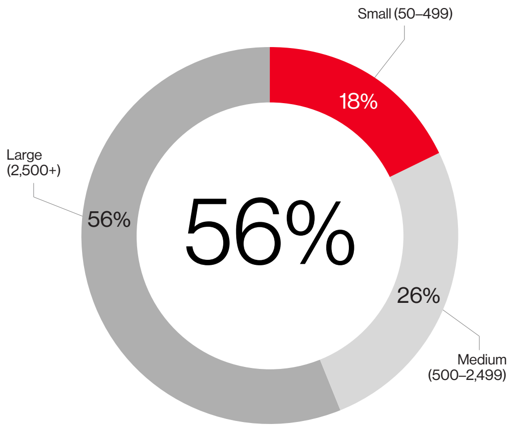


Figure 22: Organization size

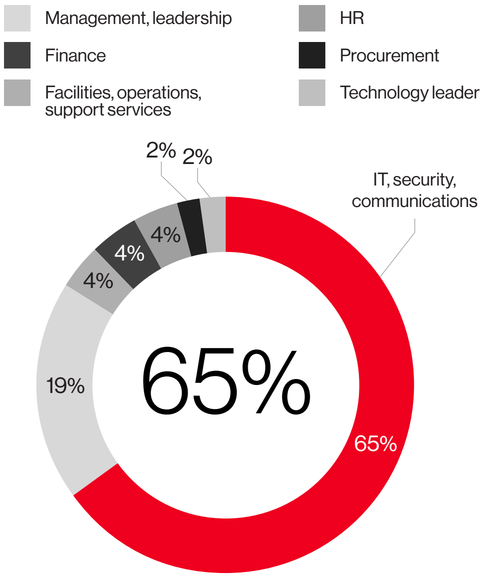


Figure 23: Role function

Contributors

We'd like to thank all our contributors for helping us to present a more robust picture of the cybersecurity threats that can affect mobile devices and the work being done to help mitigate these threats. This report wouldn't be possible without them.

CHECK POINT™

Check Point Software Technologies Ltd. is an AI-powered, cloud-delivered cybersecurity platform provider and has been providing best-in-class security solutions for more than 30 years. Because of Check Point's third-party tested prevention rates of 99.9% and 99.7% for malware and phishing, respectively, the company is consistently recognized as a leader in the cybersecurity industry, securing more than 100,000 SMB, enterprise and Public Sector organizations globally.

Check Point is known for comprehensive and integrated security solutions across networks, clouds, applications, users, and mobile and IoT/OT devices, with a focus on AI-driven and automated security.

ivanti

Ivanti Inc. is a global enterprise IT and security software company dedicated to unlocking human potential by managing, automating and protecting data and systems to empower continuous innovation. With adaptable software solutions tailored to customer needs, Ivanti empowers IT and security teams to enhance operational efficiency, cut costs and proactively mitigate security risks. The AI-powered Ivanti Neurons platform transforms the way IT and security teams operate. By delivering unified, reusable services and tools, the platform helps ensure consistent visibility, scalability and secure solution implementation, enabling teams to work smarter, not harder.

Ivanti follows "Secure by Design" principles to provide software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing risk.

Lookout™

Lookout Inc. is a globally recognized cybersecurity leader that delivers advanced protection for the most vulnerable element of any enterprise security strategy—human error and manipulation. Cloud-native by design, the Lookout platform offers rapid, scalable deployment and simplified security operations, defending the front line of human-centric attacks—the mobile device.

Lookout Mobile Endpoint Detection and Response (Mobile EDR) continuously monitors mobile endpoints for signs of human-centric attacks, as well as traditional malware, software vulnerabilities and other anomalous activity. It uses advanced threat detection techniques, including AI and behavioral analysis, to identify threats before they escalate across the enterprise.

Learn more

For additional resources and on-demand webinars from the Verizon 2025 Mobile Security Index, visit **verizon.com/mobilesecurityindex**.

And to assess your organization's mobile security readiness or speak with a Verizon expert, contact us at **verizon.com/business/contact/request-consultation**.