

2025 AFRICAN PERSPECTIVES ON CYBER SECURITY



YOU
DESERVE
THE BEST
SECURITY

C O N T E N T S

FOREWORD	04
EXECUTIVE SUMMARY	05
REGIONAL DIRECTOR REPORT	10
CYBERSECURITY IN AFRICA - OVERVIEW	13
COUNTRY MANAGER REPORTS (X4)	15
Industry focus (Financial Services, Government, Education and Telecommunications)	
• South Africa	19
• Morocco	23
• Kenya	27
• Nigeria	32
CHANNEL AND PARTNER INSIGHTS	37
BUILDING AFRICA'S CYBERSECURITY RESILIENCE	39
How Africa can overcome cybersecurity challenges by implementing Check Point solutions	40
Harnessing Africa's youth to address Africa's cyber security challenges	42
How AI is changing the game	44
PREDICTIONS	46
CONCLUSIONS & ADDENDUM	53
GLOSSARY OF TERMS	57

LORNA HARDIE

Regional Director, Africa
Check Point Software Technologies



FOREWORD

Africa is entering a defining phase of its digital transformation. From financial inclusion and e-government to smart infrastructure and education, technology is driving new levels of growth, connectivity, and opportunity. Yet this same acceleration is expanding the continent's attack surface faster than many organisations can secure it.

The findings of the 2025 report highlight this duality: innovation and exposure now move in parallel. Cyberattacks across Africa are becoming faster, more targeted, and increasingly powered by artificial intelligence. Criminals are using automation and deepfakes to breach defences, while enterprises and governments race to adopt the same technologies for progress. At Check Point, we believe Africa can leapfrog traditional cybersecurity models by embracing a prevention-first, AI-driven, and collaborative approach. Securing the connectivity fabric that powers our economies, fostering an open platform for regional partnership, and embedding AI-first security into every system will ensure innovation and safety advance together.

Resilience is not only a technical objective, it is an economic and social one. The path forward depends on shared responsibility — between public and private sectors, between nations and their partners. Together, we can build a digital future where Africa's growth is both fast and secure.



AFRICA'S DIGITAL SUCCESS WILL DEPEND ON TRUST — TRUST BUILT THROUGH PREVENTION, INTELLIGENCE, AND COLLABORATION.



EXECUTIVE SUMMARY

AFRICA'S CYBER SECURITY: THREATS, TRENDS & RESILIENCE

It is with clear intent and renewed urgency that Check Point presents the 2025 African Perspectives on Cyber Security Report. This edition shines a light on the distinct challenges and fast-evolving threats, offering evidence-based insights and practical guidance to help leaders strengthen resilience and safeguard essential services.

Africa's digital economy continues to accelerate. Payments, citizen services, education, and connectivity are scaling at pace and with that growth comes a broader attack surface. In 2025, the story is not only the volume of threats but their speed and precision. Social engineering is amplified by generative AI, identity is the new perimeter, and supply chains, from cloud to last-mile connectivity are firmly in scope.

This report is designed to help leaders cut through noise and act with confidence. It brings together regional telemetry, incident learnings, and practitioner guidance, packaged into sector and country spotlights. The aim is practical: highlight where risk is rising, what controls matter most, and how to prioritise limited resources for the greatest reduction in exposure.

Ransomware remains one of the most formidable cyber threats in Africa. The continent has witnessed a substantial increase in ransomware attacks over the past year, with more than 5,000 victims reported in 2023 alone. These attacks often exploit zero-day vulnerabilities, enabling cybercriminals to compromise numerous organisations simultaneously. The high costs associated with these vulnerabilities highlight the lucrative nature of ransomware operations.

TOP FIVE FINDINGS FOR 2025

- 1. The acceleration gap** — Africa's digital growth continues to outpace security maturity, creating opportunities for identity-led intrusions.
- 2. AI as a double-edged sword** — generative and agentic AI amplify both attack capability and defensive potential.
- 3. Critical infrastructure under pressure** — OT and IoT networks in energy, telecoms, and public services face persistent targeted attacks.
- 4. Partnerships drive resilience** — MSSPs and channel ecosystems are now essential to closing the regional skills and response gap.
- 5. Regulation and trust converge** — NIS2 and national frameworks are reshaping governance and raising market-access expectations.

GUIDING THE RESPONSE: CHECK POINT'S FOUR PRINCIPLES

All insights in this report are framed around Check Point's Four Guiding Principles, which define cybersecurity in the AI era:

- 1. Securing the Connectivity Fabric** — unified visibility and protection across cloud, mobile, OT, and data.
- 2. Prevention-First** — stopping attacks before they cause disruption or loss.
- 3. Open Platform** — enabling collaboration and integration across partners, vendors, and ecosystems.
- 4. AI-First Security** — using AI to prevent attacks, while securing AI systems from manipulation and abuse. These principles are more than a framework; they are a blueprint for Africa's next decade of secure digital growth.

AFRICA'S CYBERSECURITY BY THE NUMBERS

Metric	Africa (Avg.)	Global Avg.	Key Insight
Weekly cyberattacks per organisation	3,153	1,963	Attack pressure in Africa is among the highest worldwide.
Year-on-year increase in attack volume	-6.4%	+4.6%	Africa's attack volume average dips, masking the real trend: a shift from volume to threat sophistication
Primary exploit class	Information Disclosure: 77%	61 %	Misconfigurations and exposed data remain the top risk.
Malicious file delivery via email	80%	58 %	Email remains the dominant initial access vector.
Most targeted countries	Ethiopia, Mauritius, Zimbabwe, Uganda, Ghana	-	Regional threat landscape spans both public and private sectors.
Ransomware share of major incidents	41 %	32 %	Data-leak extortion replaces encryption as the main lever.
Avg. time to detect and contain a breach	18 days	12 days	Shortage of skilled responders delays recovery.
Most common attacker origins	Russia, Iran, China, Nigeria	-	Mix of global APTs and local criminal groups.

Source: Check Point Research (cp<r>), ThreatCloud AI Telemetry, Jan–Sep 2025.

METHODOLOGY AND SOURCES

This report draws on data from Check Point Research (cp<r>), the global threat intelligence division of Check Point Software Technologies. It combines telemetry from ThreatCloud AI, which analyses over 200 billion indicators daily, with regional insights from incident response, Managed Security Service Providers (MSSPs), and public-sector collaborations.

Data Scope

- **Time frame:** January – September 2025
- **Coverage:** 54 African countries (focus: South Africa, Nigeria, Kenya, Morocco, Egypt)
- **Events analysed:** Approx. 200 million network and endpoint detections per week
- **Sources:** ThreatCloud AI sensors, Infinity Platform telemetry, cp<r> research, partner MSSPs, open-source intelligence, and government advisories.

METHODOLOGY

1. Trend analysis of attack vectors, malware families, and exposure patterns.
2. Comparative benchmarking against global data sets.
3. Qualitative insight from Check Point regional experts and partners.
4. Predictive modelling using AI-driven threat forecasting.

Integrity and Privacy

All data is anonymized and aggregated. Analyses are validated by cp<r> analysts to ensure regional accuracy. No identifiable customer information is included.

Our guidance is prevention-first and reality-checked. Strong identity foundations, secure-by-default cloud configurations, attack-surface reduction, and well-rehearsed incident response remain the bedrock. Consolidating overlapping tools, applying threat intelligence to policy, and automating detection and response can materially shorten time-to-contain. None of this replaces people: continuous training and clear operating rhythms turn controls into capability.

Thank you to our clients, partners, and contributors across the continent who shared data and experience. Your collaboration makes this report more useful for everyone who builds, runs, and protects Africa's digital services.

We hope these insights help you ask better questions, make faster decisions, and strengthen resilience for the year ahead.

LORNA HARDIERegional Director: Africa
Check Point Software Technologies**REGIONAL REPORT**

DIGITAL GROWTH CONTINUES TO OUTPACE SECURITY

In 2025, Africa's digital expansion continues to outpace security maturity across many organisations. Cloud-first delivery, mobile money at scale, and always-on citizen services have widened the attack surface. Adversaries are escalating identity-centric intrusions, weaponizing AI to sharpen social engineering, and exploiting supply-chain gaps across SaaS providers, MSPs, and telecoms. The outcome: faster breaches, broader operational disruption, and rising verification and recovery costs for defenders.

To support leaders in this environment, Check Point's 2025 outlook distils the key threat trends and attack patterns, with sector-specific insights for Finance, Government, Education and our newest addition, Telecommunications.

SECTOR SNAPSHOTS:

- Finance: Highest exposure to identity takeover, APP fraud, and data-exfiltration-led extortion. Priorities: strong customer authentication, transaction-risk analytics, privileged-access controls, and immutable, tested backups.
- Government: Citizen data and e-services targeted by phishing, credential stuffing, and DDoS. Priorities: identity assurance for staff and vendors, API security, and layered DDoS defence with clear escalation runbooks.

- Education: Phishing and ransomware exploit distributed users and BYOD. Priorities: secure email and web gateways, patch baselines, device health enforcement, and simple, rehearsed incident response.
- Telecommunications: Attacks seek leverage at scale via core infrastructure and third-party platforms. Priorities: segmentation around crown jewels, key management hygiene, supply-chain assurance, and high-capacity DDoS controls.

WHAT'S NEW IN 2025

- AI-enabled social engineering: more convincing lures, synthetic voice/video, and personalised pretexting raise verification costs for both citizens and staff.
- SaaS sprawl: sensitive data is now widely distributed; posture management and data-loss controls for SaaS are as critical as cloud-infrastructure baselines.
- Exposure-led defence: organisations that continuously inventory internet-facing assets, remediate high-impact misconfigurations, and remove stale identities show measurable risk reduction.

CYBERSECURITY IS NOW A CONTRACTUAL GATE TO MARKET ACCESS

In addition to the cyber security challenges, Europe's Network and Information Security Directive 2 (NIS2) is now a legal requirement across the European Union (EU). Member states were required to transpose the Directive by October 17, 2024. Enforcement has accelerated through 2025, even as the Commission presses lagging countries to complete transposition. For African exporters and service providers, this changes the terms of trade.

The EU remains Africa's top trading partner. Any supplier touching European value chains, from energy and transport to manufacturing, financial services, healthcare, agriculture and digital infrastructure, will increasingly be asked to evidence NIS2-aligned controls. Non-compliance risks delayed tenders, lost contracts and heightened audit scrutiny.

THE 2025 REALITY: UNEVEN TRANSPOSITION, RISING EXPECTATIONS

Not every EU state finished transposition on time, but that does not soften buyer expectations. The Commission has opened infringement actions, and sector regulators are leaning on

CHAPTER 2

guidance and the 2024 Implementing Regulation, which hardens technical requirements for cloud, data centres, MSP/MSSP and other digital providers. These are often the same firms that African organisations partner with.

Africa's digital momentum isn't slowing, and neither are adversaries or buyer expectations. In 2025, resilience and compliance are now prerequisites for market access, especially with NIS2 shaping procurement across EU value chains. The organisations that win will treat cybersecurity as a product requirement, not a back-office function.

CYBERSECURITY IN AFRICA

OVERVIEW

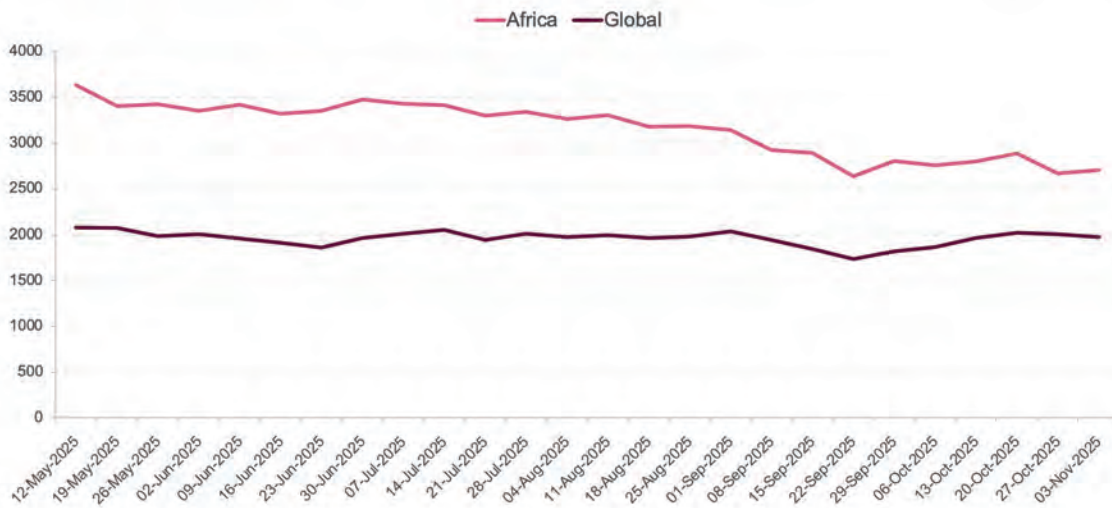
Across Africa, organisations are operating under sustained and elevated cyber pressure. Over the past six months, on average an organisation has faced 3,153 attack attempts per week, compared with 1,963 globally.

Information Disclosure remains the most common exploit class in the region, impacting 77% of organisations. Email continues to be the dominant delivery vector, with 80% of malicious files arriving via email.

Identity-centric intrusions, data-leak extortion, and exploitation of edge and cloud misconfigurations are shaping risks.

OVER THE PAST SIX MONTHS, ON AVERAGE AN ORGANISATION IN AFRICA HAS FACED 3,153 ATTACK ATTEMPTS PER WEEK, COMPARED WITH 1,963 GLOBALLY.

Attacks per Organization - Last 6 Months



THREAT LANDSCAPE: KEY TRENDS AND SOLUTIONS

CYBER WARS SET CONDITIONS FOR FUTURE ATTACKS

State-aligned operators are combining AI-driven disinformation, disruptive malware, and hacktivism to weaken trust and prepare the ground for follow-on access.

What to do: Protect public-facing services with DDoS and integrity controls and align monitoring to government and critical-infrastructure themes.

RANSOMWARE PIVOTS TO DATA-LEAK EXTORTION

Law-enforcement pressure has fragmented RaaS ecosystems, shifting affiliates to exfiltrate first and encrypt selectively.

What to do: Block data staging, inspect outbound traffic, and plan executive communications for extortion without encryption.

INFESTEALERS SURGE AND FUEL INITIAL ACCESS

Credential-stealing malware is up sharply, targeting browser tokens and VPN credentials, especially in BYOD contexts.

What to do: Deploy browser protection, bind tokens, enforce phishing-resistant MFA for admins, and accelerate credential rotation after any suspected infection.

EDGE DEVICES BECOME THE FRONT DOOR

Attackers increasingly exploit routers, VPNs, and IoT/OT to build operational relays and pivot inward.

What to do: Run aggressive firmware lifecycles, segment by default, and monitor management planes for anomalous activity.

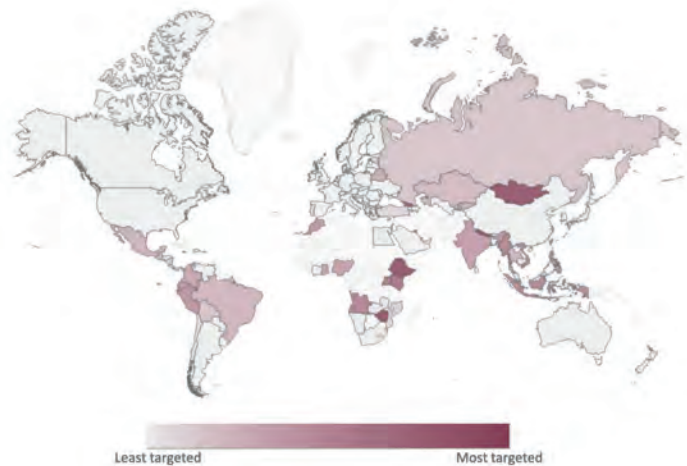
CLOUD EXPOSURE THROUGH MISCONFIGURATIONS AND API GAPS

Hybrid complexity and reliance on external SSO create lateral paths between on-prem and cloud.

What to do: Use CSPM/CNAPP to detect drift, secure secrets, and apply least-privilege, with guardrails for LLM/AI service use.

REGIONAL SNAPSHOT & RECENT NOTABLES

- #1 Ethiopia
- #2 Mauritius
- #3 Zimbabwe
- #4 Uganda
- #5 Ghana



MOST TARGETED COUNTRIES (SEPTEMBER 2025)

ATTACK VECTORS AND FILE DELIVERY (LAST 30 DAYS):

Email dominates malware delivery in Africa, accounting for 80% of malicious files. Prioritise email security, payload sandboxing, and user isolation for high-risk roles.

BRAND PHISHING (Q2 2025):

Attackers used convincingly branded pages impersonating a global music streaming service to harvest credentials and payment details. Treat third-party payment flows and single-sign-on redirects as high-risk and monitor for look-alike domains.

MAJOR ATTACKS & DATA BREACHES IN AFRICA

SEP 2025: GOOGLE SECURITY UPDATE FOR GOOGLE CHROME

Google releases security update for Google Chrome, addressing CVE-2025-9478, a critical use after free vulnerability in ANGLE.

SEP 2025: CPR GLOBAL REPORT

Check Point Research shows global cyber threats in agriculture surge by 101% in August 2025. Africa has highest weekly attack rates.

AUG 2025: SEYCHELLES COMMERCIAL BANK

Exposure of 2.2GB of sensitive customer and staff data, including personal and account information.

JUN 2025: STEALTH FALCON ESPIONAGE

Zero-day exploited via malicious .url files and WebDAV delivery; targeting government and defence across the Middle East and Africa with multi-stage implants.

MAY 2025: SOUTH AFRICAN AIRWAYS

Cyberattack disrupted web, mobile, and some internal systems; core operations remained unaffected pending data-exposure assessment.

APR 2025: MTN (SOUTH AFRICA)

Unauthorised access to personal information for some customers; critical infrastructure and customer services unaffected while investigation proceeded.

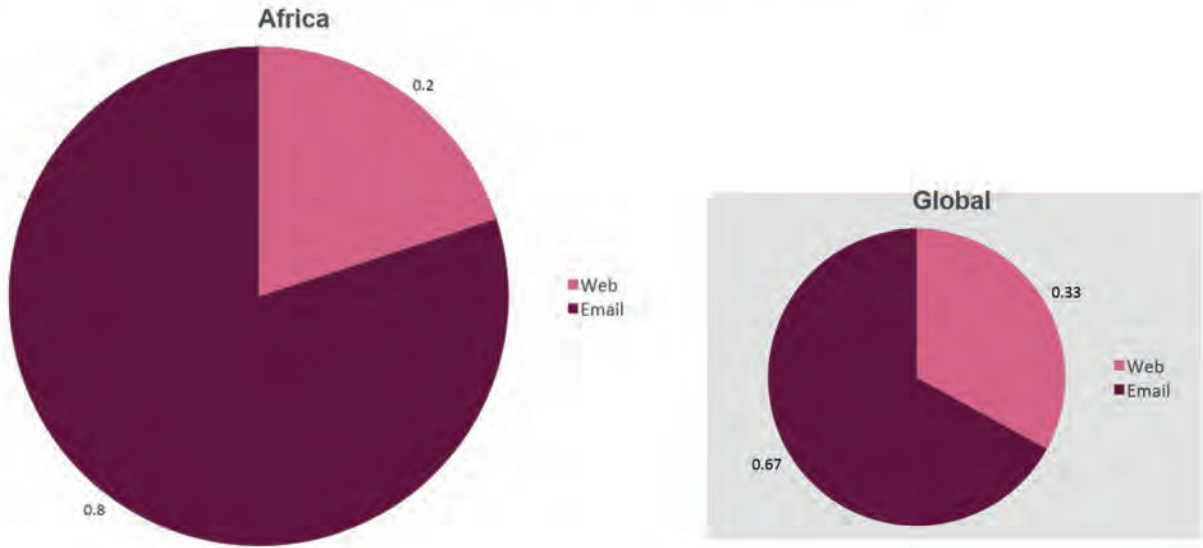
APR 2025: MOROCCO CNSS

Breach claimed by an Algerian group with alleged theft of personal and financial information and a related government website defacement.

FEB 2025: SHADOWPAD/NAILOLOCKER ACTIVITY

Adversaries exploited CVE-2024-24919 (patched May 2024) in a campaign active through January 2025, impacting organisations in Africa among other regions.

Attack Vectors for Malicious Files- Last 30 Days



LIONEL DARTNALL

Country Manager, East Africa
Check Point Software Technologies



SOUTH AFRICA 2025: DEFENDING TRUST IN THE AGE OF AI-ENABLED ATTACKS

South Africa's cybersecurity landscape has entered an era defined by AI-powered deception and relentless exposure. The nation remains one of the most targeted markets on the continent, facing a complex mix of legacy vulnerabilities, rapid digital adoption, and an expanding threat surface that mirrors its economic growth. Over the past year, threat actors have leveraged artificial intelligence, automation, and cloud misconfigurations to execute faster, more adaptive campaigns, forcing organisations to redefine what resilience truly means.

Check Point telemetry reveals that South African entities face thousands of attacks weekly, with phishing, data exfiltration, and DDoS activity dominating the threat spectrum. Botnets like Vo1d and XorDDoS continue to infect enterprise and consumer devices, fuelling smishing and ransomware operations

Yet the deeper threat lies in the erosion of digital trust itself, where deepfakes and synthetic communications are blurring the boundaries between authentic and fake AI shifting the battleground. Cyber criminals now wield generative models to bypass verification systems and impersonate trusted identities. Check Point's AI-aware defence frameworks, powered by Lakera's AI-native protection stack, detect and neutralise AI-driven deception in real time, ensuring that South African enterprises can innovate without fear of compromise.

Meanwhile, Continuous Threat Exposure Management (CTEM) and External Risk Management (ERM) are becoming central to South Africa's defensive posture

By continuously scanning for vulnerabilities, exposed credentials, and brand misuse, organisations can now move from reacting to anticipating, turning intelligence into prevention. Cybersecurity in 2025 is not about hardening walls; it's about rebuilding trust at digital speed.

THREAT LANDSCAPE IN 2025

Over the last six months, organisations faced 2,116 attack attempts per week on average, compared with 1,963 globally.

GOVERNMENT A PERSISTENT TARGET

Government remains a persistent target in South Africa. The sector's top threats are ransomware with data-leak extortion and infostealers used to harvest credentials. Active families shaping adversary tradecraft include Qilin, Akira, and Play. The most frequently exploited weakness is Information Disclosure, which impacts 76% of South African organisations, and is often compounded by edge-device weaknesses and cloud/API misconfigurations.

EDUCATION UNDER PRESSURE

Higher education and research remain vital to national growth and a consistent target set for credential theft and data exposure. Institutions experience sustained pressure broadly aligned with the national average with seasonal surges around academic cycles.

The most common threats are infostealers and botnet-delivered loaders for credential harvesting, followed by targeted data-leak extortion after mailbox compromise. Key vulnerabilities include academic email and SSO misconfigurations, exposed tokens, and over-permissive data shares that lead to Information Disclosure.

FINANCIAL SERVICES DRAWS ATTENTION

Banking, insurance, and payments underpin the economy and draw continuous attention from organised cybercrime. Globally, this sector sees persistent targeting of approximately 1,701 attacks per organisation per week, with periodic spikes around payment cycles and public events.

Top threats include infostealers harvesting VPN and session tokens; ransomware affiliates focusing on data theft and selective encryption; and credential-stuffing and API abuse against consumer portals. Common weaknesses include edge-device exposures, cloud/API misconfigurations, and dependence on external SSO, which increases the blast radius of token theft.

TELECOMMUNICATIONS IDENTITY ABUSE

Telecommunications providers in South Africa operate under sustained pressure. The primary risks are identity abuse and API exposure on consumer portals, alongside ransomware actors favouring data-leak extortion and infostealers that harvest tokens from BYOD/VPN contexts.

The sector's most common weakness mirrors the international picture: Information Disclosure exposures affect 78% of organisations and are often compounded by edge-device weaknesses (VPN/SSL gateways, routers) and cloud/API misconfigurations. This number refers to Global Telecommunications, there is insufficient data on this industry in South Africa.

MAJOR ATTACKS AND DATA BREACHES

The picture is consistent: attackers targeted consumer-facing digital channels and identity paths; core operations were not disrupted, but investigations and assurance work are ongoing. For leadership, the takeaway is to harden identity and API surfaces, tighten edge controls, and be ready to communicate quickly if customer data is implicated.

April 2025 - MTN South Africa

MTN South Africa confirmed a cybersecurity incident involving unauthorised access to personal information of some customers. The company stated that critical infrastructure and customer services remained unaffected while the incident was investigated. The immediate focus included containment, validation of access controls on customer portals and APIs, and customer notification where required.

The case underscores the risk of token theft and API misuse in high-scale consumer environments and the value of short-lived sessions, strict conditional access, and robust monitoring around identity providers.

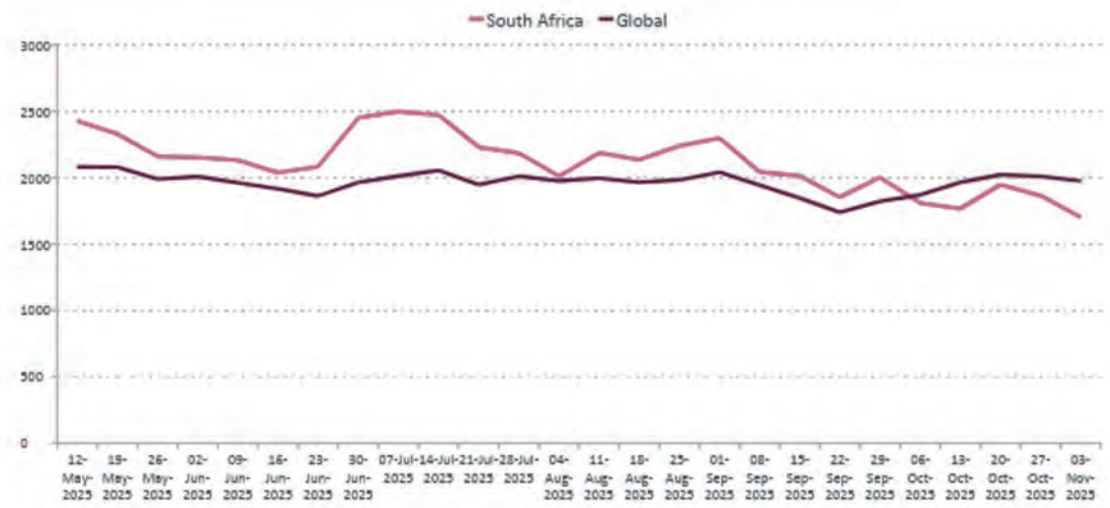
May 2025 - South African Airways (SAA)

South African Airways experienced a cyberattack that disrupted its website, mobile app, and

some internal systems. The incident was quickly contained, and core flight operations were unaffected. An investigation is underway to determine whether any customer or employee data was exposed.

The event highlights the operational importance of keeping digital customer channels resilient, maintaining immutable backups for web and application platforms, and rehearsing incident communications that address potential data-exposure concerns.

Attacks per Organization - Last 6 Months



MHAMMED DINNIA

Country Manager North Africa,
Check Point Software Technologies



MOROCCO 2025: ELEVATED CYBER PRESSURE, IDENTITY-LED INTRUSIONS

Morocco has become a pivotal player in North Africa's digital expansion, but with connectivity and innovation has come exposure. The nation continues to face persistent and coordinated attacks targeting government institutions, education networks, transport infrastructure, and the financial sector.

Recent intelligence from Check Point's External Risk Management Services (ERMS) revealed large-scale campaigns by Keymous + MA and RootSec MA, whose DDoS assaults and defacements sought to disrupt core systems and undermine public confidence

These attacks highlight the risks of accelerated digital transformation without equivalent investment in cyber hygiene. Phishing, credential theft, and brand impersonation remain dominant vectors, while vulnerabilities in web applications and misconfigured servers continue to open doors to intrusion. As Morocco positions itself as a bridge between Africa and Europe, ensuring cyber maturity has become a strategic imperative.

Continuous Threat Exposure Management (CTEM) is reshaping Morocco's approach to resilience. By continuously mapping the nation's external attack surface, CTEM empowers organisations to detect exposed credentials, misconfigurations, and vulnerabilities before they are exploited. Paired with Check Point's prevention-first architecture, this transition turns reactive security into predictive defence.

Artificial intelligence now magnifies both opportunity and risk. Adversaries are weaponizing AI to automate phishing, create synthetic identities, and exploit model weaknesses

Check Point's AI-native technologies, strengthened through its acquisition of Lakera, enable Moroccan enterprises to innovate confidently by protecting their data, models, and users in real time. Morocco's cybersecurity journey in 2025 is defined by vigilance, intelligence, and alignment, proving that resilience is strongest when it never sleeps.

THREAT LANDSCAPE IN 2025

Morocco's digital economy is expanding fast, and so are the stakes. Over the last six months, organisations in Morocco faced 2 317 attack attempts per week on average, compared with 1 963 globally. Information Disclosure is the most common exploit class, impacting 69% of organisations.

Phishing-led campaigns continue to drive credential theft, with brand-impersonation lures observed in Q3 2025, alongside rising misuse of edge devices and exposed APIs. The signal for leaders is clear: harden identity, web, and email controls together, and close configuration gaps across cloud and edge.

Morocco sits firmly in the sights of both state-aligned and financially motivated actors. Nation-state operations increasingly use AI-driven disinformation, disruptive malware, and hacktivism to weaken trust and prepare the ground for follow-on access. Criminal groups continue their pivot from encryption to **data-leak extortion**, while **infostealers** have surged, harvesting browser tokens and VPN credentials, especially in BYOD contexts. Attackers also target **edge devices** to create relay infrastructure and pivot into networks, and **cloud/API misconfigurations** remain a common route to sensitive data.

What this means for you: Expect credential-led intrusions, data staging, and lateral movement across hybrid estates. Prioritise token hygiene and short-lived sessions, rapid patching of internet-facing systems (including collaboration platforms), and continuous posture management across cloud services.

GOVERNMENT A PERSISTENT TARGET

Government remains a persistent target in Morocco. While activity varies with the civic calendar, pressure remains high. The sector's top threats are ransomware with data-leak extortion and infostealers used to harvest credentials, often followed by exploitation of collaboration systems and exposed APIs. Globally, the most frequently exploited weakness is

Information Disclosure (69% of organisations), compounded by edge-device weaknesses and cloud/API misconfigurations.

EDUCATION UNDER PRESSURE

Higher education and research are critical to Morocco's growth and remain consistent targets for credential theft and data exposure. Institutions face sustained pressure, with surges around academic cycles. The most common threats are infostealers and botnet-delivered loaders for credential harvesting, followed by targeted data-leak extortion after mailbox compromise. Key vulnerabilities include academic email and SSO misconfigurations, exposed tokens, and over-permissive data shares that lead to Information Disclosure.

FINANCIAL SERVICES DRAWS ATTENTION

Banking, insurance, and payments underpin Morocco's economy and draw continuous attention from organised cybercrime. Targeting remains persistent, with periodic spikes around payment cycles and public events.

Top threats include infostealers harvesting VPN and session tokens; ransomware affiliates focusing on data theft and selective encryption; and credential-stuffing and API abuse against consumer portals. Common weaknesses include edge-device exposures, cloud/API misconfigurations, and dependence on external SSO, which increases the blast radius of token theft.

TELECOMMUNICATIONS IDENTITY ABUSE

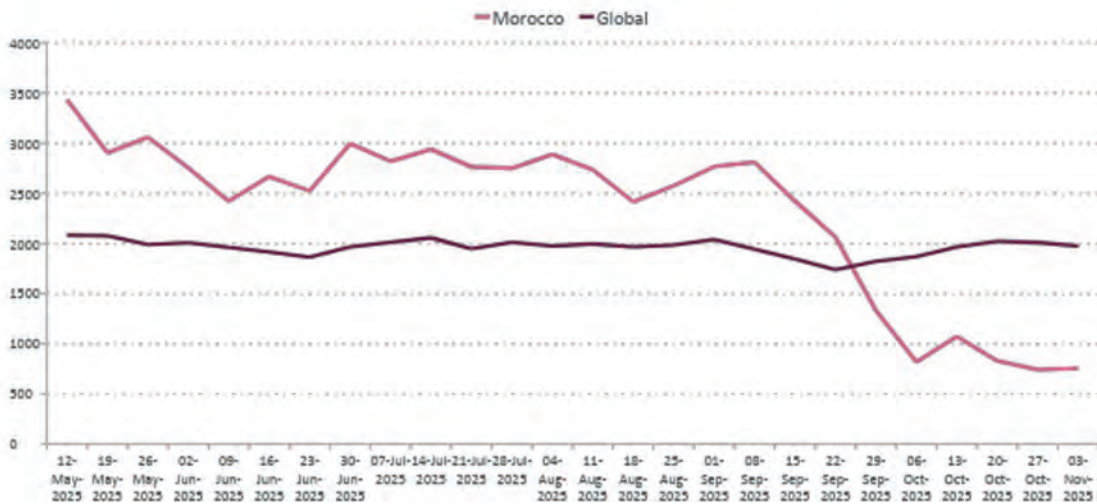
Morocco's telecom operators face sustained pressure. Risk is driven by identity misuse and exposed APIs on customer-facing channels, with ransomware crews prioritising data-leak extortion and widespread infostealer infections siphoning browser and VPN tokens, especially in BYOD/VPN contexts.

The dominant weakness is Information Disclosure (seen across 78% of organisations globally), and it is amplified by fragile edge appliances, from VPN/SSL gateways to access routers, and by cloud/API configuration drift. Q2 2025 also saw credible brand-phishing lures (for example, music-streaming look-alikes), reinforcing the need for tighter email/web controls and scrutiny of payment and sign-in flows.

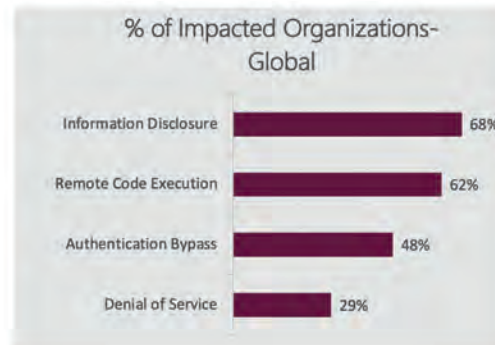
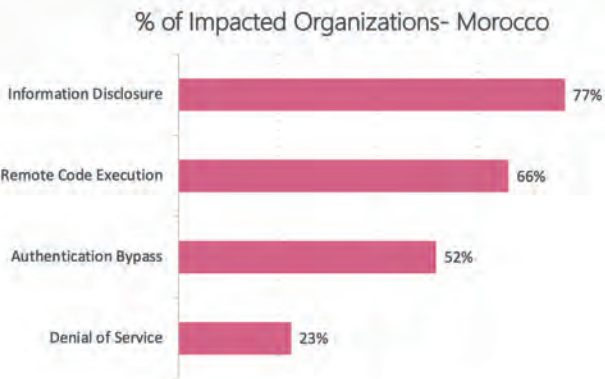
MAJOR ATTACKS AND DATA BREACHES

April 2025: CNSS (Morocco’s Social Security Institute). An Algerian group (JabaROOT) claimed a breach affecting personal and financial information for up to 2 million citizens and defaced a government website. The case underscores the importance of SSO hardening, rapid credential rotation, and robust DLP and egress monitoring across public-facing services.

Attacks per Organization - Last 6 Months



Top Vulnerability Exploit types - Last 30 Days



JOHN PAUL ONYANGOCountry Manager: East Africa,
Check Point Software Technologies

KENYA 2025: HIGH ATTACK VOLUME, RCE-LED INTRUSIONS

Kenya's position as East Africa's digital powerhouse comes with both pride and peril. Kenya faced 3,758 attack attempts per week on average, compared with 1 963 globally. The most common vulnerability exploit type in Kenya is Information Disclosure, impacting 77% of the organizations.

The dominant exploit class is Remote Code Execution (RCE), impacting 70% of organisations.

The country's embrace of mobile banking, fintech innovation, and digital government has accelerated national growth, but also expanded the attack surface dramatically. In 2025, ransomware, phishing, and operational-technology (OT) disruptions dominate Kenya's threat landscape, targeting systems that form the backbone of its economy.

Check Point ERMS intelligence highlights a new wave of attacks against critical sectors. The Qilin ransomware group targeted KenGen and Uganda's UETCL, demonstrating how cybercriminals are now merging OT sabotage with data theft.

These campaigns reflect a strategic shift from quick financial gain to prolonged disruption, designed to undermine public trust in essential infrastructure.

To stay ahead, Kenyan enterprises are adopting Continuous Threat Exposure Management (CTEM), a framework that continuously maps vulnerabilities, prioritises remediation, and validates defences before adversaries strike.

This proactive visibility transforms cybersecurity into an operational discipline, enabling CISOs to measure and mitigate exposure in real time.

AI adds urgency to this evolution. Generative models are being used to craft credible phishing content, impersonate executives, and infiltrate identity systems

To counter this, Check Point's AI-native security technologies, integrated into the Infinity architecture, safeguard data and models with precision and speed. Kenya's next chapter will be defined by coordination, between government, enterprise, and technology, to build a digital economy where innovation is protected by trust.

THREAT LANDSCAPE IN 2025

Kenya's threat picture mirrors global shifts. Nation-state operators are using AI-assisted disinformation, disruptive malware, and hacktivism to erode trust and set conditions for future access. Ransomware affiliates are emphasising data-leak extortion over encryption. Infostealers have surged, harvesting browser and VPN tokens, especially in BYOD environments, and feeding initial-access brokers.

Adversaries are also turning edge devices into relay infrastructure and exploiting cloud/API misconfigurations to move laterally between on-prem and cloud estates. A notable 2025 signal is widespread exploitation of Microsoft SharePoint CVE-2025-53770, initially focused on government, software and telecommunications, and later expanding to financial services.

What this means for you: Patch public-facing services fast, including collaboration platforms, shorten session lifetimes and rotate risky tokens, and enable outbound inspection to stop data staging and exfiltration. Validate cloud posture continuously and harden API authentication and authorisation flows.

GOVERNMENT A PERSISTENT TARGET

Government agencies remain attractive to both state-aligned and financially motivated actors. RCE-class flaws and collaboration-platform exposures (including SharePoint CVE-2025-53770) are high-probability entry points. Expect infostealer-led credential abuse, followed by data-leak extortion attempts. Focus on rapid patch SLAs, phishing-resistant MFA for admins, and segmentation around sensitive citizen-data systems.

EDUCATION UNDER PRESSURE

Higher education and research continue to face consistent pressure from infostealers and botnet-delivered loaders that harvest credentials and tokens, with targeted data-leak extortion following mailbox compromise. Common gaps include SSO/email misconfigurations, exposed tokens, and over-permissive data shares that convert into RCE and lateral-movement risk across academic platforms.

FINANCIAL SERVICES DRAWS ATTENTION

Banks, insurers, and payments providers draw persistent attention from organised cybercrime. Infostealers that capture VPN/session tokens remain a primary on-ramp, while credential-stuffing and API abuse target consumer portals. The SharePoint CVE-2025-53770 exploitation wave broadened to include financial services, raising the priority of collaboration-platform hardening, customer-identity protection, and strict network segmentation between digital channels and core processing.

TELECOMMUNICATIONS IDENTITY ABUSE

Telcos face sustained risk across customer-facing portals and management planes. Identity misuse and exposed APIs drive incidents, while ransomware crews lean on data-leak extortion and pervasive infostealer infections siphon tokens from BYOD/VPN contexts. Given the 2025 exploitation of SharePoint CVE-2025-53770, telecom operators should enforce token hygiene, conditional access, and rigorous patch SLAs for internet-facing collaboration and support systems.

MAJOR ATTACKS AND DATA BREACHES

August 2025: Seychelles Commercial Bank (Africa). A data breach exposed approximately 2.2 GB of sensitive customer and staff data, including names, dates of birth, phone numbers, account types, balances, and records linked to government officials, impacting both individual and business accounts.

What this means for you: treat correspondent-banking and third-party connections as high-risk paths; tighten DLP and identity monitoring around cross-border payment systems.

August 2025: Orange (Telecom, France). A cyberattack caused operational disruptions affecting French customers and select business and consumer services. Investigators reported no evidence of customer or company data exfiltration at the time of reporting, and the extent of any compromise remains unclear.

What this means for you: continuity plans for customer portals and network management should account for service-degrading attacks even without data loss.

August 2025: Tea (Global consumer app). A breach exposed roughly 59 GB of sensitive user data, including 72,000 images (selfies, government IDs, and in-app photos) and a separate database containing 1.1 million private messages exchanged between members.

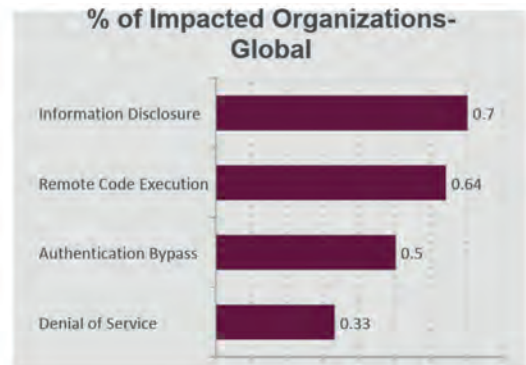
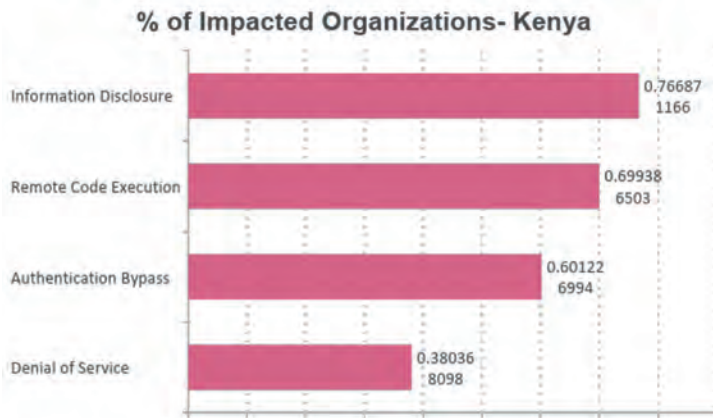
What this means for you: assume recycled credentials and ID-document leakage will drive fraud attempts; increase credential-stuffing defences and verification checks.

August 2025: Pi-hole (Open-source/IT). Due to a vulnerability in the GiveWP WordPress donation plugin, donor names and email addresses of nearly 30,000 supporters were exposed.

What this means for you: third-party plug-ins and community platforms are supply-chain risks; enforce patch cadences and monitor for list-harvesting-driven phishing.

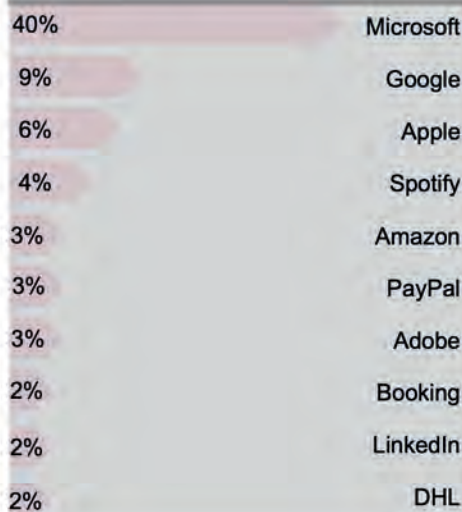
August 2025: Aeroflot and Russian pharmacy chains. Pro-Ukrainian hacktivist groups triggered major operational disruptions—severe flight delays at Aeroflot and widespread outages at Stolichki and Neofarm. The attackers claim database exfiltration (flight history, workstation data, call recordings, personnel monitoring data) and allege wiping of 7,000 servers (22 TB).

Top Vulnerability Exploit types - Last 30 Days



Brand Phishing – Q3 2025

Top Brands



Top industries

- 1 Technology
- 2 Social Networks
- 3 Retail

In Q3, a malicious phishing site operating under the domain `paypal-me[.]icu`, designed to impersonate the **PayPal** brand. This fake site leveraged social engineering tactics, offering fraudulent rewards to entice users. Once clicking to get the payment, it lures victims into inserting sensitive information such as login credentials, passwords, and credit card details.



KINGSLEY OSEGHAE

Country Manager: West Africa,
Check Point Software Technologies



NIGERIA 2025: BUILDING TRUST IN AN ERA OF RELENTLESS ATTACKS

Nigeria's digital economy continues to expand at speed, and with that momentum comes intensified cyber pressure. Financial services, telecoms, and emerging sectors such as energy and healthcare are facing sustained, high-volume attacks. Nigerian organisations now record an average of 4 200 attack attempts per week, more than double the global average, confirming that adversaries are scaling as fast as digital transformation itself.

The financial sector remains the epicentre of these threats. Phishing and Business Email Compromise persist as dominant entry points, proving that awareness and training are just as vital as technology. Beyond finance, energy and healthcare operators are integrating IoT and cloud-based systems, creating efficiencies but also new vulnerabilities. As global oil majors divest to local players, cybersecurity governance must transfer with ownership, or risk inheriting invisible threats.

Encouragingly, Nigeria's cybersecurity maturity is rising. Organisations are deploying layered prevention-first architectures across perimeter, endpoint, and cloud environments. Many now rely on Check Point to protect both production and disaster recovery systems, recognising that true resilience demands continuity as much as control.

AI, however, is rewriting the playbook. Attackers use automation and deep learning to accelerate compromise, forcing defenders to match speed with intelligence

Check Point's integrated Infinity architecture, combined with Laker's AI-native runtime

protection, gives Nigerian enterprises a decisive advantage, securing data, identities, and applications across the attack surface. The challenge ahead is clear: close configuration gaps, strengthen identity controls, and turn cybersecurity into a shared national discipline of trust.

THREAT LANDSCAPE IN 2025

Nigeria's threat picture aligns with global shifts. Nation-state operators leverage AI-assisted disinformation, disruptive malware, and hacktivism to weaken trust and set conditions for access. Ransomware affiliates emphasise data-leak extortion over encryption, and infostealers have surged, harvesting browser and VPN tokens (especially in BYOD) to feed initial-access brokers. Adversaries increasingly convert edge devices into relay infrastructure and exploit cloud/API misconfigurations to move laterally. A notable 2025 signal is widespread exploitation of Microsoft SharePoint CVE-2025-53770, initially focused on government, software, and telecommunications, and later expanding to financial services.

What this means for you: Patch public-facing services fast (including collaboration platforms), shorten session lifetimes and rotate risky tokens, enable outbound inspection to stop data staging and exfiltration, and validate cloud posture and API auth flows continuously.

GOVERNMENT: RCE-EXPOSED & CREDENTIAL-LED

Government entities remain high-value targets for both state-aligned and financially motivated actors. Expect infostealer-led credential abuse and data-leak extortion attempts, with collaboration-platform exposures (including SharePoint CVE-2025-53770) as likely entry points.

Priorities: rapid patch SLAs, phishing-resistant MFA for admins, and segmentation around citizen-data systems.

EDUCATION: INFOSTEALERS, BOTNET LOADERS & MAILBOX-LED

Higher education and research institutions face consistent pressure from infostealers and botnet-delivered loaders that harvest credentials and tokens, with targeted data-leak extortion following mailbox compromise. Common gaps include SSO/email misconfigurations, exposed tokens, and over-permissive data shares that increase lateral-movement risk across academic platforms.

FINANCIAL SERVICES: TOKEN THEFT, API ABUSE & RCE SPILLOVER

Banks, insurers, and payments providers draw persistent attention from organised cybercrime. Infostealers that capture VPN/session tokens remain a primary on-ramp, while credential-stuffing and API abuse target consumer portals. The SharePoint CVE-2025-53770 exploitation wave expanded to financial services, raising the priority of collaboration-platform hardening, customer-identity protection, and strict segmentation between digital channels and core processing.

TELECOMMUNICATIONS: IDENTITY MISUSE & COLLAB-PLATFORM

Telcos face sustained risk across customer-facing portals and management planes. Identity misuse and exposed APIs drive incidents, while ransomware crews lean on data-leak extortion and pervasive infostealer infections siphon tokens from BYOD/VPN contexts. Given 2025 SharePoint exploitation, telecom operators should enforce token hygiene, conditional access, and rigorous patch SLAs for internet-facing collaboration and support systems.

MAJOR ATTACKS & DATA BREACHES (2025)

August 2025: Seychelles Commercial Bank (Africa). A data breach exposed approximately 2.2 GB of sensitive customer and staff data, including names, dates of birth, phone numbers, account types, balances, and records linked to government officials, impacting both individual and business accounts.

What this means for you: treat correspondent-banking and third-party connections as high-risk paths; tighten DLP and identity monitoring around cross-border payment systems.

August 2025: Orange (Telecom, France). A cyberattack caused operational disruptions affecting French customers and select business and consumer services. Investigators reported no evidence of customer or company data exfiltration at the time of reporting, and the extent of any compromise remains unclear.

What this means for you: continuity plans for customer portals and network management should account for service-degrading attacks even without data loss.

August 2025: Tea (Global consumer app). A breach exposed roughly 59 GB of sensitive user data, including ~72,000 images (selfies, government IDs, and in-app photos) and a separate database containing 1.1 million private messages exchanged between members.

What this means for you: assume recycled credentials and ID-document leakage will drive fraud attempts; increase credential-stuffing defences and verification checks.

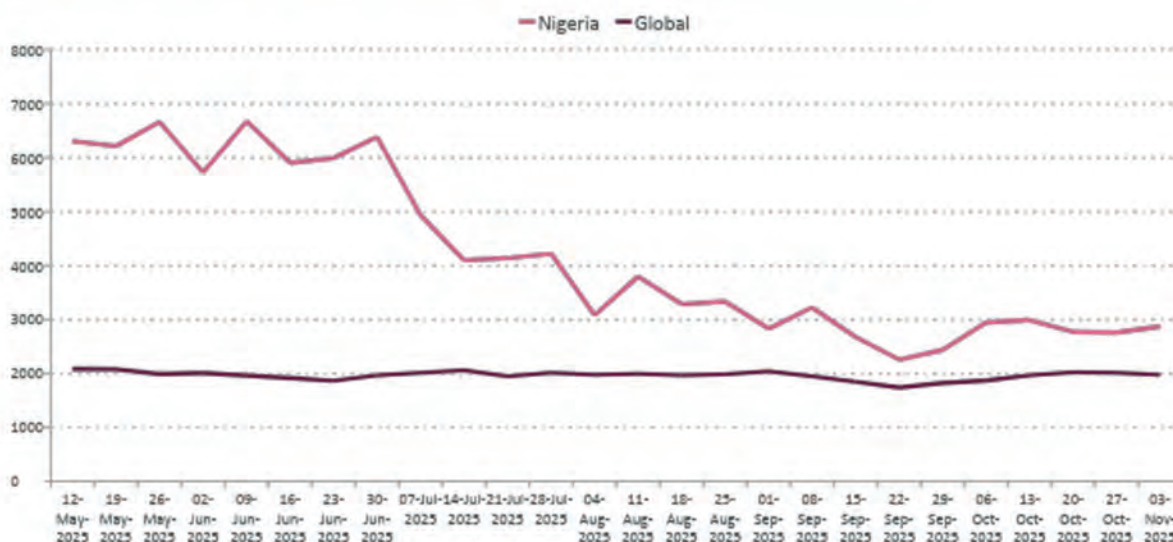
August 2025: Pi-hole (Open-source/IT). Due to a vulnerability in the GiveWP WordPress donation plugin, donor names and email addresses of nearly 30,000 supporters were exposed.

What this means for you: third-party plug-ins and community platforms are supply-chain risks; enforce patch cadences and monitor for list-harvesting-driven phishing.

August 2025: Aeroflot and Russian pharmacy chains. Pro-Ukrainian hacktivist groups triggered major operational disruptions, severe flight delays at Aeroflot and widespread outages at Stolichki and Neofarm. The attackers claim database exfiltration (flight history, workstation data, call recordings, personnel monitoring data) and allege wiping of 7,000 servers (22 TB).

What this means for you: plan for geopolitical spillover and destructive scenarios; rehearse incident communications and fallback operations when primary systems are degraded.

Attacks per Organization - Last 6 Months

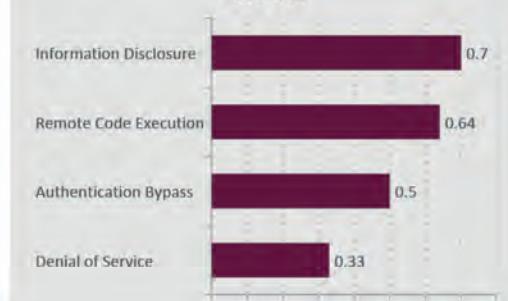


Top Vulnerability Exploit types - Last 30 Days

% of Impacted Organizations- Nigeria

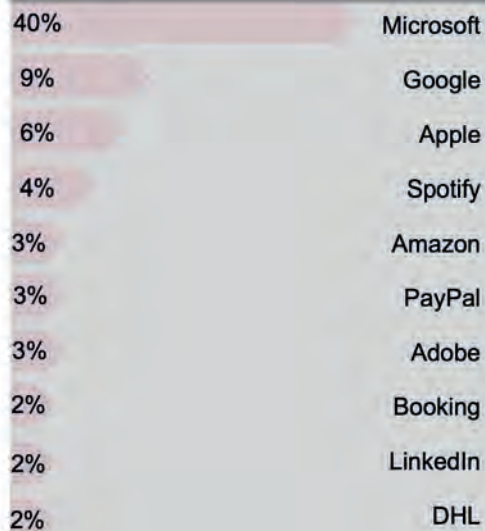


% of Impacted Organizations- Global



Brand Phishing – Q3 2025

Top Brands



Top industries

- 1 Technology
- 2 Social Networks
- 3 Retail

In Q3, a malicious phishing site operating under the domain paypal-me[.]icu, designed to impersonate the **PayPal** brand. This fake site leveraged social engineering tactics, offering fraudulent rewards to entice users. Once clicking to get the payment, it lures victims into inserting sensitive information such as login credentials, passwords, and credit card details.

1,00 €

PayPal

VINCENT MABASO

Channel Manager: Africa,
Check Point Software Technologies



CHANNEL INSIGHTS: BUILDING AFRICA'S CYBER ECOSYSTEM

As Africa's leading markets continue to face escalating and sophisticated cyber pressure, the continent's resilience increasingly depends on the strength of its partnerships. Behind every successful defence strategy lies a network of local channel partners translating technology into trust, adapting global innovation to local realities, and ensuring that prevention-first cybersecurity reaches every organisation that needs it.

Africa's cybersecurity resilience depends not only on technology but on the strength of the ecosystem delivering it. Channel partners and distributors sit at the centre of this reality, the human and operational bridge between innovation and implementation. Their proximity to customers, market insight, and ability to tailor solutions for local contexts make them the true multipliers of Check Point's impact across the continent.

In 2025, Check Point's channel strategy focuses on three long-term priorities: enablement, profitability, and differentiation. The aim is to move beyond transactional sales toward genuine solution alignment, helping partners deliver value that is sustainable, measurable, and prevention-first. This approach ensures that every deployment strengthens both the customer's posture and the partner's business model.


Check Point's Open Garden Hybrid Mesh framework remains pivotal to this ecosystem. It allows customers to integrate Check Point's AI-led defences into their existing cybersecurity investments without replacement, creating a flexible and cost-efficient path to modernisation.

This adaptability is particularly valuable in Africa, where organisations often operate with diverse legacy systems and tight budgets but still face enterprise-grade threats.

Channel incentives have also evolved. Partners are now rewarded for the depth and quality of engagement, not just sales volume, encouraging lifecycle management, renewal excellence, and customer retention. By staying close to the customer, understanding sector-specific pain points, and addressing niche needs from financial compliance to telecom-grade identity assurance, Check Point's partners are redefining what local cyber resilience looks like.

Across the region, success stories reflect this shift. From Cybyl in Kenya and FPG Technologies in Nigeria to Data Group in South Africa, partners are demonstrating how collaboration and knowledge-sharing translate into tangible outcomes, expanded pipelines, faster deployment cycles, and measurable reductions in client exposure.

The next phase for Africa's cybersecurity ecosystem will be defined by how effectively vendors, partners, and customers intentionally learn and build together. For Check Point, the goal is clear: empower a channel that doesn't just sell security, but delivers trust at scale.



BUILDING AFRICA'S CYBER RESILIENCE

Africa's attack pressure remains among the highest globally, and identity exposure is rising, pushing credentials to the centre of most compromises. The priority for leaders is clear: reduce the opportunities attackers have to log in rather than break in, contain data movement, and shorten the time from detection to response.

What's changed in 2025. Ransomware has tilted toward data-leak extortion; exploitation of collaboration platforms (including new SharePoint flaws) has accelerated; education sees seasonal phishing waves; and operators are experimenting with AI-assisted social engineering.

HOW AFRICA CAN OVERCOME CYBERSECURITY CHALLENGES WITH CHECK POINT

Make credential exposure visible and fix it fast. Use External Risk Management (ERM) to discover leaked employee credentials across open, deep and dark-web sources, prioritise by business impact, and trigger automated rotation/takedown. Pair ERM with Harmony Email & Collaboration so identity risks emerging from email compromises surface and can be resolved immediately.

Treat web and email as one control plane. While the continent remains email-heavy, digital leaders like South Africa see a higher share of web-borne threats. Unify prevention across email, web, endpoint and SaaS so phishing payloads, token theft and session replay are blocked consistently. Add browser-level protections for high-risk roles and short-lived sessions for admins.

Shut the doors attackers actually use. Prioritise patch SLAs on internet-facing systems (including collaboration platforms); enforce phishing-resistant MFA for admins; bind tokens to devices; and restrict management planes on edge devices (VPN/SSL gateways, routers). In the cloud, run continuous posture management to stop misconfig drift and over-privilege before it becomes data exposure.

Design for containment and recovery. Assume exfiltration-first ransomware. Classify and monitor sensitive data with inline DLP and outbound inspection; keep backups immutable and offline; perform timed restores; and rehearse executive communications for leak-based extortion.

ARCHITECTURE PRIORITIES FOR SOLUTION-AGNOSTIC OUTCOMES

- **One policy, many planes:** Consistent prevention across endpoint, network, edge, and cloud, informed by unified threat intelligence.
- **Identity-first security:** Conditional access, device trust, token binding, and short-lived sessions for sensitive roles.
- **Data-centric controls:** Classification, tagging, and movement controls across SaaS/LaaS with monitored egress.
- **AI/LLM guardrails:** Scrub secrets, enforce provenance, and control model egress to prevent inadvertent data leakage.

BOARD PRIORITIES: RISK, INVESTMENT & ASSURANCE

- **Risk narrative:** Credential-led intrusions and data-leak extortion threaten operations and regulatory exposure across multiple sectors.
- **Investment asks:** Edge lifecycle budget, email and browser protection, cloud posture automation, immutable backup and recovery, and IR readiness.
- **Assurance:** Quarterly attack-path reviews and tested recovery objectives (RPO/RT0) with executive buy-in.

ACTION PLAN CHECKLIST

- **Patch & validate collaboration platforms under active exploitation,** e.g., Microsoft SharePoint CVE-2025-53770; confirm admin controls and access logs are locked down.
- **Harden identity:** enforce phishing-resistant MFA for admins; rotate/revoke risky tokens quickly; shorten high-privilege session lifetimes (infostealers/credential theft trend).
- **Tighten email + web together:** enforce DMARC/SPF/DKIM; enable advanced phishing detection/sandboxing; monitor for brand-phishing lures (Q3'25 examples).
- **Fix cloud/API misconfigurations** via continuous posture management and least-privilege; review third-party SSO/API dependencies (hybrid exposure theme).

- **Secure edge devices** (VPN/SSL gateways, routers): patch aggressively; close exposed management interfaces; monitor management planes (edge-device targeting).
- **Block data-leak extortion** with inline DLP and outbound inspection to stop staging/exfiltration (ransomware shift to leaks).
- **Assure recovery:** keep immutable, offline backups for critical systems and perform timed restores (extortion resilience).

HARNESSING AFRICA'S YOUTH TO CLOSE THE SKILLS AND AWARENESS GAP

Africa's young, mobile-first population is both a prime target and a powerful defence multiplier. TikTok adoption is deep among youth (with more than 60% of users aged 16–24), and platform subcultures like “ScamTok” glamorise quick-win fraud techniques. That narrative is reinforced by localised “hustle” groups (e.g., Nigeria's Yahoo/BM Boys) that flaunt stolen wealth to recruit peers.

The combination of high mobile penetration in cities (often above 95%), informal tech learning (YouTube/forums), and limited formal online-safety training (under 40% of youth receiving it) widens exposure. Reporting remains low across the continent: only a small fraction of victims alert police or banks, with many defaulting to friends/family or staying silent due to embarrassment. The result is under-reported harm and faster social spread of scam playbooks.

WHAT'S DRIVING VULNERABILITY

- **Economic pressure & opportunity gaps:** Hundreds of thousands of young people enter labour markets annually with limited formal jobs; “fast-money” scams are positioned as a shortcut.
- **Peer & platform dynamics:** FOMO, social shaming, and creator influence normalise risky behaviour; recruitment flows through friendship circles, gaming communities and chat groups.

- **Always-online behaviour:** Rapid context-switching across apps widens the attack surface; “how-to” videos package illicit tactics as tech tips.
- **Limited deterrence:** Cross-border attacks and scarce specialist units lower the perceived cost of offending; victims rarely report through official channels.

WHAT TO PUT IN PLACE (PRACTICAL MOVES)

- **Cyber Ambassadors** in schools/universities and community centres (local languages) to teach credential hygiene, scam recognition, and secure-by-default habits.
- **Creator & platform partnerships** to counter “ScamTok”: collaborate with trusted influencers; promote the platform’s scam-prevention resources; amplify reporting and takedown pathways.
- **Youth pipelines into cyber jobs:** ethical-hacking clubs, CTF leagues, and paid internships that feed SOC, IR, and threat-intel roles; celebrate defender stories, not scam lore.
- **Low-friction reporting & victim support:** confidential channels, clear next steps, and stigma-free messaging to raise disclosure rates.
- **Check Point’s Secure Academy** provides global cyber education to more than 250 academic institutions across 70+ countries. In Africa, it has already trained over 500 students through 19 active partnerships.

Source: <https://datareportal.com/reports/digital-2025-south-africa>

HOW AI IS CHANGING THE GAME AND HOW TO RESPOND

Ransomware crews are experimenting with AI-enabled operations (from social-engineering at scale to automated negotiation tooling) while advanced actors refine evasion, for example abusing signed drivers to disable security controls. Meanwhile, phishing operators continue to iterate brand-impersonation lures, with global tech and media brands frequently spoofed.

COUNTER-MOVES THAT WORK:

- **Automate external risk discovery** with ERM so leaked credentials, brand-impersonation sites, and exposed assets are found and fixed quickly.
- **Identity-first access:** phishing-resistant MFA, device trust, token binding, and conditional access for high-risk actions.
- **Exploit-aware patching:** prioritise collaboration platforms and internet-facing apps when exploitation is active.
- **EDR hardening:** enable driver/installer blocklists, memory protections, and tamper-proofing to counter kill-switch tactics.

A PRACTICAL CHECKLIST FOR THIS QUARTER

- Turn on **ERM** and leaked-credential alerts; rotate any exposed credentials within hours.
- Patch/validate **collaboration platforms** under active exploitation; lock down admin interfaces on edge devices.
- Enforce **DLP with outbound inspection**, alert on unusual bulk movement and token theft indicators.
- Shorten **admin session lifetimes**; bind tokens to device posture; roll out browser isolation for high-risk roles.
- Run a **data-leak extortion exercise** with legal/PR; perform a timed restore from immutable backups.

In this way, African organisations can outpace adversaries by focusing on the highest-impact levers: make leaked-credential exposure visible and fix it fast; harden identity and collaboration platforms; close misconfiguration and edge gaps; and practice recovery. Equip and mobilise youth as a safety multiplier and use automation to reduce every window of attacker opportunity.

PREDICTIONS

FROM ACCELERATION TO AUTONOMY: AFRICA'S DIGITAL TURNING POINT

The year 2026 will mark a profound turning point for Africa's cybersecurity landscape.

Artificial intelligence, automation, and hyper-connectivity are now redefining the continent's growth trajectory, accelerating economic inclusion while exposing new systemic vulnerabilities.

Across finance, energy, telecoms, and government, the same digital transformation driving prosperity is also creating an expanded attack surface. The challenge is no longer connectivity, but control: how to secure the complex, data-rich ecosystems Africa is rapidly building.

Drawing on the insights of Check Point's African leadership team, these eight predictions explore how the region's innovation, regulation, and human capital will shape a decade defined by prevention, transparency, and shared resilience.

1. AGENTIC AI BEFORE GOVERNANCE

By 2026, agentic artificial intelligence, autonomous systems capable of reasoning and acting without human oversight, will be deeply embedded in workflows across logistics, finance, and public administration.

Globally, this evolution is transforming productivity, but it also exposes a governance gap: when AI systems act independently, who is accountable for their outcomes?

Across Africa, countries like Kenya, Nigeria, and South Africa have drafted national AI strategies, but execution and ethical oversight remain limited. Private-sector adoption, particularly in fintech and telecoms, is outpacing regulation, creating opportunities for efficiency but also for misuse and bias.

Embedding governance early, through transparency, audit trails, and explainable AI, will determine whether Africa leads responsibly or reacts belatedly.

Why it matters: Governance will determine whether AI accelerates inclusion or amplifies inequality.

Reference: [B20 South Africa 2025 – Responsible AI Agenda](#)

2. DEEPFAKE FRAUD BECOMES MAINSTREAM

AI-generated deception is becoming the fastest-growing cyber threat. The convergence of generative AI and mobile platforms is blurring the line between authentic and synthetic identity.

In Africa's mobile-first economy, where over 650 million people use mobile devices for finance and communication, deepfake scams can bypass authentication entirely.

SIM-swap and identity fraud already cost South Africa over R5 billion annually. The next wave of attacks will involve impersonation, fake executive calls, cloned voice approvals, or synthetic customer interactions. This evolution threatens to undermine not just individuals, but public confidence in digital systems.

Why it matters: When every image or voice can be faked, proof replaces perception as the cornerstone of security.

Reference: [TransUnion Africa Digital Fraud Report 2025](#)

3. CLOUD MISCONFIGURATIONS OVERTAKE MALWARE

As African organisations modernise, cloud platforms are becoming mission critical. Yet misconfigurations, not malware, cause the majority of breaches worldwide.

According to the World Economic Forum's Global Cyber Outlook 2025, 60% of global cloud incidents result from human error or permission drift.

Africa's hybrid infrastructures, often managed by small security teams or external integrators, are especially exposed. The problem is not adoption but oversight: unmonitored APIs, unpatched test environments, and inconsistent governance.

Why it matters: In 2026, configuration hygiene will matter more than antivirus. The unseen will cause the most damage.

Reference: [ITWeb Africa – Cloud Risk 2025](#)

4. DATA EXTORTION TARGETS CRITICAL INFRASTRUCTURE

Ransomware has evolved into data-pressure operations, exfiltrating and threatening to leak sensitive information rather than encrypting it. Africa's critical infrastructure, from aviation to utilities, is increasingly in the crosshairs.

Incidents at Seychelles Commercial Bank and South African Airways have demonstrated how attackers exploit operational technology for leverage.

As [*industrial digitalisation grows 30% year-on-year*](#), the consequences extend beyond downtime to public trust. A corrupted dataset in a transport or energy grid can trigger cascading real-world disruption.

Why it matters: Integrity, not availability, will be the new measure of resilience.

Reference: [*Engineering News – Infrastructure Exposure 2025*](#)

5. EXTERNAL RISK SCORES BECOME BOARD KPIS

Cybersecurity has become a board-level discipline. By 2026, external risk ratings and exposure scores will influence investment, creditworthiness, and regulatory standing.

[*The African Union's Digital Security Framework*](#) is pushing for transparency in reporting cyber posture across member states.

As executives seek quantifiable metrics, cybersecurity will join financial and ESG performance as a marker of corporate maturity.

Why it matters: What the board measures, the business secures.

Reference: [*TechCentral – Cyber Visibility on African Boards*](#)

6. EXTERNAL RISK SCORES BECOME BOARD KPIS

The convergence of the [EU's NIS2 Directive](#), the AI Act, and global data regulations is reshaping international trade.

African exporters in manufacturing, fintech, and cloud services will need to demonstrate compliance as a condition for market access. Non-compliance could delay tenders or exclude firms from lucrative cross-border contracts.

Compliance has become a performance metric, demonstrating trust in real time rather than through paperwork.

Why it matters: Regulation is evolving from paperwork to performance, resilience is the new trade currency.

Reference: [European Commission – NIS2 Directive](#)

7. THE SKILLS GAP BECOMES A NATIONAL CRISIS

The global cybersecurity talent shortage has surpassed five million, and Africa represents a critical share.

Despite its young, digitally fluent population, the continent still has over 200,000 unfilled cybersecurity roles. Without local expertise, reliance on external providers will deepen.

Initiatives like [Smart Africa's Digital Academy](#) and regional cyber labs are making progress, but scale and sustained funding remain essential.

Why it matters: Cyber sovereignty begins with skills, without human capacity, even the best tools fail.

Reference: [Tech Africa News – Skills Gap and Scam Economy](#)

8. MSSPS BECOME AFRICA'S RESILIENCE ENGINE

Managed Security Service Providers (MSSPs) are rapidly becoming Africa's operational backbone.

The shortage of in-house expertise and constrained budgets are driving small and mid-sized enterprises toward managed defence models. By 2026, most will consume cybersecurity "as a service."

This shared-resilience model enables continuous protection through AI-assisted analytics and centralised threat intelligence, bridging skill, visibility, and coverage gaps.

Why it matters: MSSPs democratise advanced defence, bridging both talent and tooling gaps.

Reference: [Connecting Africa – Partnerships Power Cyber Defence](#)

9. IDENTITY BECOMES THE NEW ECONOMY

As Africa accelerates toward a unified digital economy, identity is becoming the new currency of trust.

National digital ID initiatives in [Nigeria](#), [Kenya](#), and [South Africa](#) are reshaping how citizens access financial, healthcare, and government services.

By 2026, passwordless and biometric authentication will replace legacy systems, while AI-driven behavioural verification will redefine what it means to "log in."

Why it matters: Trust in digital identity will determine the future of fintech, governance, and inclusion.

Reference: [FIDO Alliance – Authentication Trends 2025](#)

FROM EXPOSURE TO ORCHESTRATION

Africa's digital future will not be defined by threats, but by tempo.

AI, automation, and hybrid infrastructures are accelerating faster than governance, yet Africa's agility gives it a unique advantage. The continent can embed security, transparency, and education into its growth story, rather than layering them on afterward.

The message is clear: prevention, partnership, and people will determine who leads the next decade of digital trust.

CONCLUSION & ADDENDUM

CONCLUSION

FROM ACCELERATION TO ASSURANCE

Africa's digital progress is unstoppable, but its sustainability depends on trust. The evidence in this report shows that prevention, collaboration, and intelligent automation are the decisive levers for that trust. Check Point's commitment is to help governments, enterprises, and partners translate these insights into measurable resilience — ensuring that as the continent connects, it also protects.



AFRICA'S NEXT LEAP FORWARD WILL BE SECURED BY DESIGN — POWERED BY PREVENTION, GUIDED BY INTELLIGENCE, AND BUILT ON SHARED RESPONSIBILITY.

LORNA HARDIE

REGIONAL DIRECTOR, AFRICA,
CHECK POINT SOFTWARE TECHNOLOGIES

ADDENDUM

TURNING INSIGHT INTO ACTION – BUILDING AFRICA’S CYBER RESILIENCE

The 2025 findings reveal a continent in rapid transition — where digital acceleration is transforming economies faster than cybersecurity maturity can keep pace. Across finance, government, telecommunications, and education, five themes now define Africa’s cyber reality.

1. **The Acceleration Gap: Digital growth continues to outstrip defensive capacity.** Hybrid networks, cloud adoption, and mobile ecosystems are expanding faster than organisations can secure them.
 - ✓ Enterprises must unify control across environments, embedding automation and prevention into every workflow.
2. **AI as Catalyst and Risk: Artificial intelligence is reshaping both attack and defence.** Generative AI enables convincing social engineering and polymorphic malware, while also empowering defenders to predict and block threats in real time.
 - ✓ Resilience depends on using AI responsibly and protecting AI models, data, and decision pipelines from manipulation.
3. **Critical Infrastructure Under Pressure: Energy, transport, and telecoms now face persistent, targeted campaigns that blend data theft with service disruption.**
 - ✓ Safeguarding operational technology requires segmentation, continuous posture management, and prevention-first protection across converged IT/OT estates.
4. **Collaboration as a Force Multiplier: Skills shortages are driving demand for Managed Security Service Providers (MSSPs) and public-private partnerships.**
 - ✓ Africa’s cybersecurity future will be shaped by open ecosystems where intelligence and accountability are shared.
5. **Regulation, Trust, and People: With frameworks such as POPIA, NDPA, and the EU’s NIS2, compliance and cyber resilience are becoming inseparable. Yet human error remains the easiest path to compromise.**
 - ✓ Investing in awareness, governance, and identity assurance delivers faster returns than reactive recovery.

THE CHECK POINT FRAMEWORK FOR ACTION

All these insights point toward a single truth: prevention must become Africa's default operating model for digital success. Check Point's Four Guiding Principles provide a practical framework for achieving that goal:

- 1. Securing the Connectivity Fabric** – unifying visibility and protection across networks, clouds, and endpoints so every connection is trustworthy.
- 2. Prevention-First** – blocking attacks before they cause damage, reducing cost and complexity for defenders.
- 3. Open Platform** – integrating with partners and MSSPs to build collective resilience across diverse infrastructures.
- 4. AI-First Security** – using AI to predict and stop threats, while securing AI systems themselves from manipulation and data leakage.

These principles are already visible in Africa's most successful cyber-mature enterprises — where prevention is embedded, not added, and security enables innovation rather than limiting it.

GLOSSARY OF TERMS

AI (Artificial Intelligence) A computer system's ability to perform tasks that normally require human intelligence, like learning or problem-solving. In cybersecurity, AI is a "double-edged sword": criminals use it to create smarter scams (like deepfakes), while defenders use it to predict and stop attacks faster.

API (Application Programming Interface) A digital "messenger" that allows different software applications to talk to each other. For example, a travel website's API might ask an airline's API for flight prices. If not secured, attackers can use APIs to steal data or abuse services.

Attack Surface The total number of all possible entry points (like employee laptops, company servers, mobile phones, and cloud apps) that an attacker could try to exploit to get into a network.

Botnet A network of computers infected with malware, controlled as a group by a single attacker (the "bot-herder") without the owners' knowledge. These "robot networks" are often used to carry out large-scale attacks, like sending spam or conducting DDoS attacks.

BYOD (Bring Your Own Device) The practice of allowing employees to use their personal devices (like their private smartphone or laptop) to connect to the company network and do work. This can be risky if those personal devices are not secure.

Cloud A general term for services (like data storage, software, or computing power) that are delivered over the internet. Instead of living on your computer, the data and programs "live" in a data center owned by companies like Amazon, Google, or Microsoft.

Credential Stuffing A type of cyberattack where a hacker takes lists of stolen usernames and passwords (leaked from a past data breach) and "stuffs" them into the login pages of many other websites, hoping to find a match. This works because many people reuse the same password.

CTEM (Continuous Threat Exposure Management) A proactive cybersecurity strategy. Instead of just waiting to be attacked, CTEM involves constantly scanning a company's own systems to find and fix security weaknesses before hackers can find them.

Cybersecurity The practice of protecting computers, networks, and data from digital attacks, theft, or damage.

Dark Web A hidden part of the internet that you can't find with regular search engines like Google. It requires special software to access and is often used for illegal activities, such as selling stolen data, drugs, or hacking tools.

Data Exfiltration The act of secretly stealing and moving data from inside a company's network to an attacker's own server.

DDoS (Distributed Denial of Service) An attack that tries to knock a website or online service offline by flooding it with an overwhelming amount of fake traffic from many different sources (often a botnet). It's like a thousand people all trying to get through a single doorway at once, blocking legitimate users.

Deepfake An AI-generated video or audio clip that realistically fakes a person's appearance or voice. Deepfakes are used in advanced scams to impersonate a CEO, politician, or family member to trick someone.

Exploit A piece of software code or a command that takes advantage of a specific bug or vulnerability (a weakness) in a system to cause an unintended effect, such as gaining control of that system.

Hacktivism Hacking that is done for a political or social cause, rather than for financial gain. This can include defacing government websites or leaking documents to protest an issue.

Identity In cybersecurity, your "identity" is the collection of data (like your username, password, and security tokens) that proves you are who you say you are online. It is the "new perimeter," meaning attackers now focus on stealing your identity rather than just breaking into a building.

Infostealer (Information Stealer) A type of malware specifically designed to scan an infected computer and steal saved information, such as passwords stored in your browser, credit card details, and crypto-wallet data.

IoT (Internet of Things) & OT (Operational Technology)

IoT: Refers to everyday "smart" devices connected to the internet, like smart watches, home security cameras, or smart refrigerators.

OT: Refers to the technology used to control and monitor physical industrial equipment, like the machinery in a factory, a power grid, or a water treatment plant. Attacks on OT are very dangerous as they can cause physical-world disruption.

LaaS (Licence-as-a-Service) A cloud-based model for managing software licenses that replaces traditional license key management.

Malware A general term for any malicious software (like viruses, ransomware, or infostealers) that is designed to disrupt, damage, or gain unauthorized access to a computer system.

Misconfiguration A human error in setting up a system's security. This is like leaving the front door of your house unlocked or a window wide open. For example, failing to put a password on a cloud database is a common misconfiguration.

MSSP (Managed Security Service Provider) An outside company that other businesses hire to manage their cybersecurity. MSSPs act as a company's remote security team, monitoring for threats and responding to incidents 24/7.

NIS2 A major cybersecurity law in the European Union (EU). It's important for African companies because any organization that does business with or provides services to EU countries must now meet these high security standards, or risk losing contracts.

Phishing A scam where an attacker sends a fraudulent email, text, or message pretending to be a legitimate person or company (like your bank or your boss) to trick you into revealing sensitive information, like a password or credit card number.

Smishing: Phishing that is done via SMS (text message).

Ransomware A type of malware that locks up (encrypts) a victim's files, making them inaccessible. The attacker then demands a ransom (a payment, usually in cryptocurrency) in exchange for the key to unlock them.

Data-Leak Extortion: A modern form of ransomware where attackers also steal your data before locking it. They then threaten to publish the sensitive data online if you don't pay.

SaaS (Software-as-a-Service) Software that you "rent" and use over the internet, rather than buying and installing it. Common examples include Microsoft 365, Google Workspace, and Salesforce.

SIM-Swap Fraud A type of identity theft where an attacker convinces your mobile phone provider to transfer your phone number to a new SIM card that they control. Once they have your number, they can intercept your calls and text messages, including one-time security codes, to take over your bank accounts.

Social Engineering The psychological manipulation of people into giving up confidential information or performing actions they shouldn't. Phishing, deepfakes, and impersonation calls are all forms of social engineering. It's essentially hacking the human, not the computer.

Supply Chain Attack An attack that targets a less-secure "supplier" to get to a bigger, more secure "customer." For example, a hacker might attack a small IT vendor to gain access to all the large corporations that vendor services.

VPN (Virtual Private Network) A tool that creates a secure, encrypted connection (a "tunnel") over the internet. It is often used by remote employees to safely connect to their company's internal network.

Zero-Day A newly discovered security weakness in a piece of software. It is called "zero-day" because the software vendor has zero days to fix it before hackers start using it to attack systems. These are very dangerous because no patch or fix exists yet.

CONTACT US

AFRICAN OFFICES

KENYA OFFICE

Check Point Software Technologies
Regus Center, Vienna Court, State House Road
Nairobi Kenya

NIGERIA OFFICE

Check Point Software Technologies
Sterling Virtual Offices
2 Turnbull street , Banana Island
Lagos Nigeria

SOUTH AFRICA OFFICE

Check Point Software Technologies, Unit 2C, Cedar Office Park,
Stinkwood Cl, Fourways,
Sandton, 2055, South Africa

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

WWW.CHECKPOINT.COM

