Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Africa. Q4 2025

16.04.2026

Version 1.0

Africa 3
Key cybersecurity issues in the region 3
Statistics across all threats 4
Threat sources 6
Internet 7
Email clients 8
Removable media 10
Threat categories 12
Self-propagating malware: worms and viruses 14
Spyware 17
Ransomware 19
Malicious scripts and phishing pages 20
Industries 21
Threat sources and malware categories in industries: 'hotspots' 27
Methodology used to prepare statistics 33

Africa

Key cybersecurity issues in the region

Low cybersecurity maturity of industrial companies

High threat detection rates point to low cybersecurity maturity across industrial companies on the continent: the availability of internet access on OT computers, weak phishing protection, large portions of unprotected infrastructure, and still relatively poor employee cyberhygiene.

In Africa, the percentage of ICS computers on which all categories of threats except miners in the form of executable files for Windows were blocked is higher than the global average**.**

Unprotected OT infrastructure and weak network segmentation

In Africa, the percentage of ICS computers blocking self-propagating malware (worms and viruses) is significantly higher than the global average. By the percentage of ICS computers on which worms were blocked, Africa leads all other regions by a wide margin; in terms of viruses, it ranks second.

High detection rates of self-propagating malware and malware spread via network folders at the industry, country, or regional level likely indicate unprotected OT infrastructures lacking even basic endpoint protection. Such unprotected computers become sources of further malware spread.

Weak enterprise network segmentation and lack of control over removable media further exacerbate the situation.

Absence or ineffectiveness of perimeter defenses for OT networks

The rate of spyware detections in the region far exceeds the global average: it was 1.6 times higher in Q4 2025.

Finding spyware on ICS computers usually indicates that the initial infection vector — whether a malicious link, an attachment from a phishing email, or an infected USB device — has already succeeded. This points to the lack or ineffectiveness of OT network perimeter defenses, such as monitoring network communications and enforcing removable media usage policies.

By the percentage of ICS computers on which spyware was blocked, Africa consistently ranks first among all regions.

Lack of control over the use of removable media

In Q4 2025, the percentage of ICS computers on which threats from removable media were blocked was 4.5 times higher than the global average. In this indicator, Africa leads the world by a wide margin.

Frequent attempts to infect protected systems via USB drives may indicate:

- A low level of enterprise digitalization (lack of secure internal file storage and transfer systems);
- The existence of significant unprotected enterprise infrastructure acting as a source of USB infections;
- A poor overall information security culture.

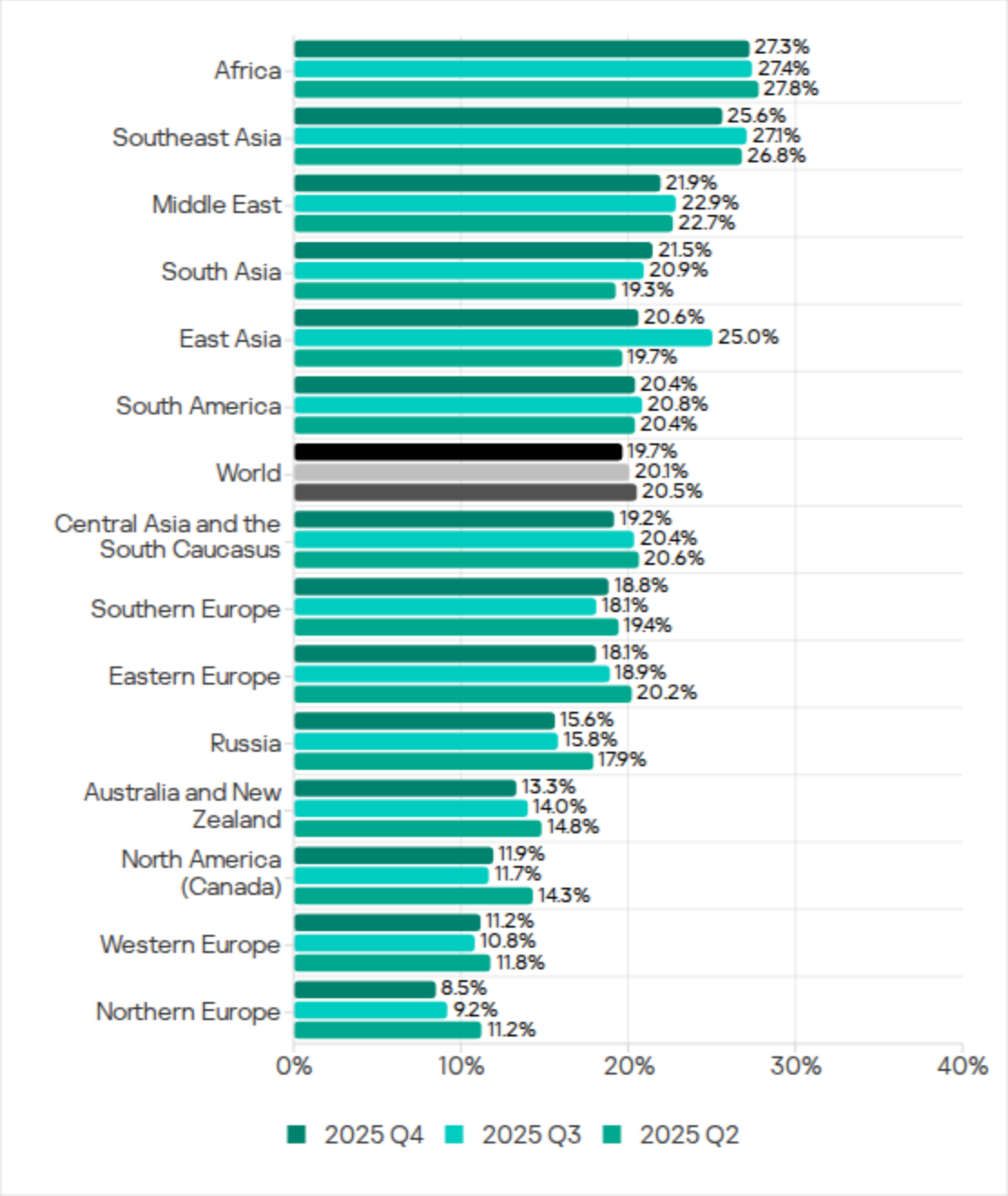
Cybersecurity adoption lags behind the pace of rapidly developing industries

One broad conclusion we can draw from years of monitoring OT infrastructure exposure to threats is that the implementation of cybersecurity measures and tools almost always lags behind industry growth. When facilities are commissioned, cybersecurity is often an afterthought. Protections are insufficient, staff is poorly trained, and compliance with security policies is half-hearted.

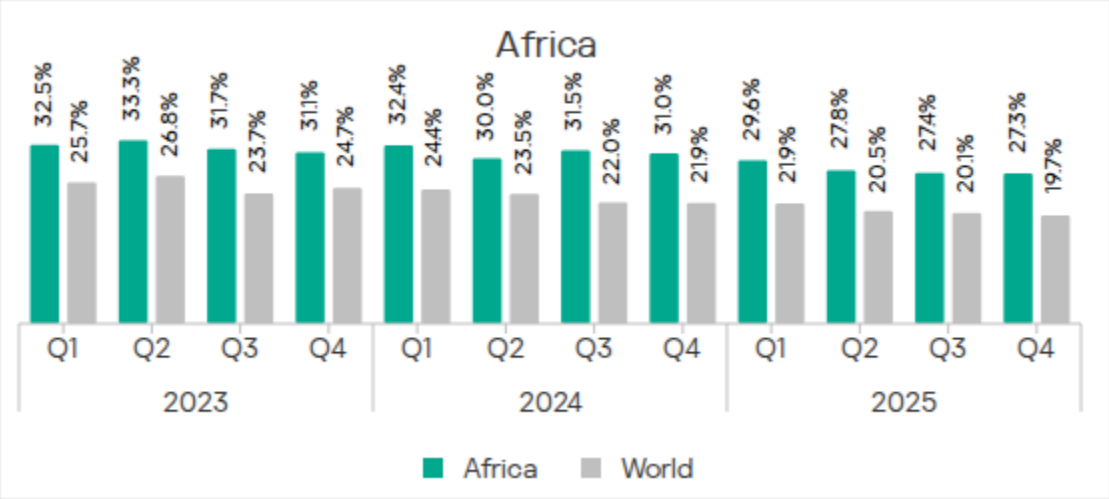
This trend is clearly visible in statistics on African industries and infrastructure types (see below). Rapidly developing sectors include oil and gas, energy, manufacturing, and construction. Engineering is developing alongside these.

Statistics across all threats

In Q4 2025, Africa remained the leading region by percentage of ICS computers on which malicious objects were blocked, with a figure that was still 1.4 times higher than the global average.

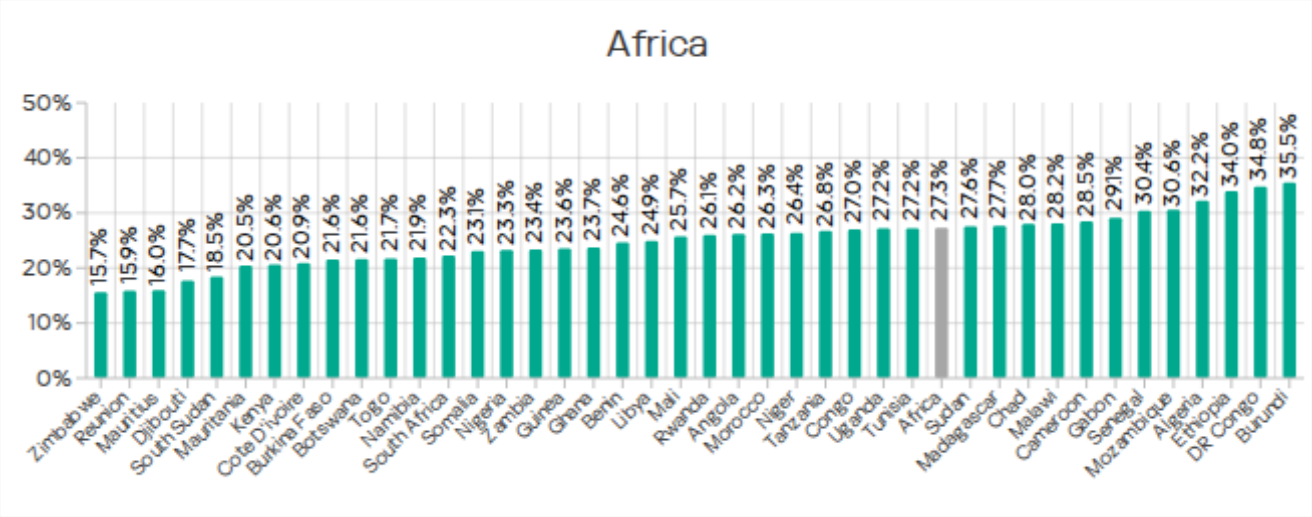


This indicator has declined in the region for five consecutive quarters, reaching 27.3%. This is 3.2 times higher than in Northern Europe, the region with the lowest ranking.



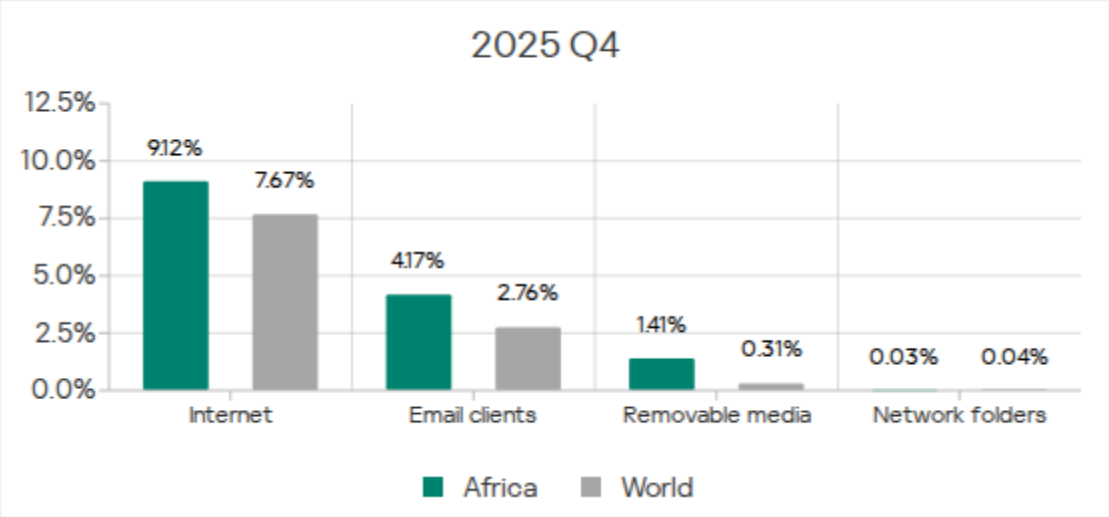
The percentage of ICS computers on which malicious objects were blocked in African countries ranged from 15.7% in Zimbabwe to 35.5% in Burundi, where the figure increased by as much as 7 pp in Q4 2025.

Only three countries had a rate below 20%: Zimbabwe, Mauritius, and Djibouti. In Senegal, Mozambique, Algeria, Ethiopia, the DRC, and Burundi, the rate was over 30%.

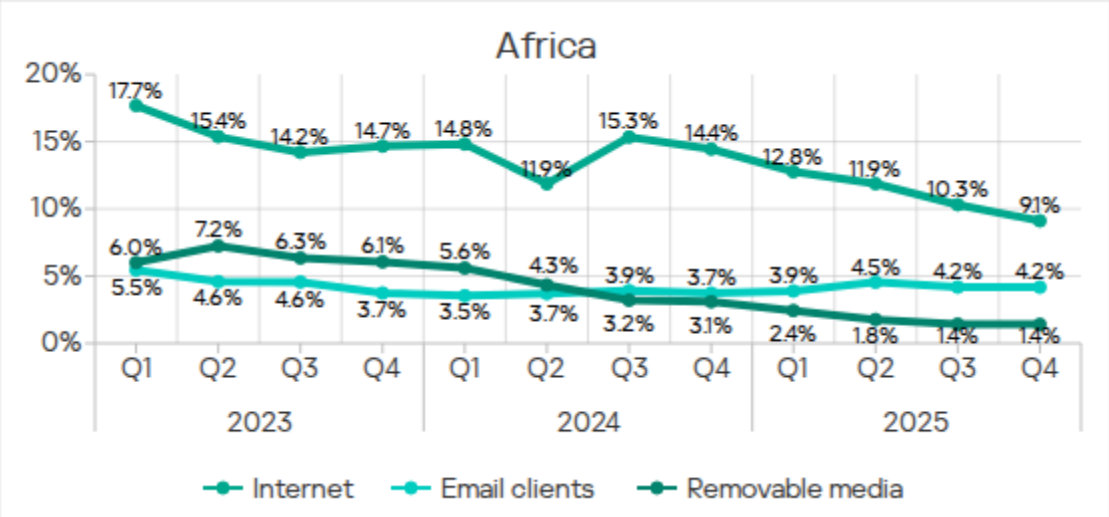


Threat sources

In Q4 2025, the rate in Africa was higher than the global average for all threat sources, except for network folders. The rate for removable media threats was particularly high, at 4.5 times higher. The rate for internet threats was 1.2 times higher than the global average, while the rate for email client threats was 1.5 times higher.



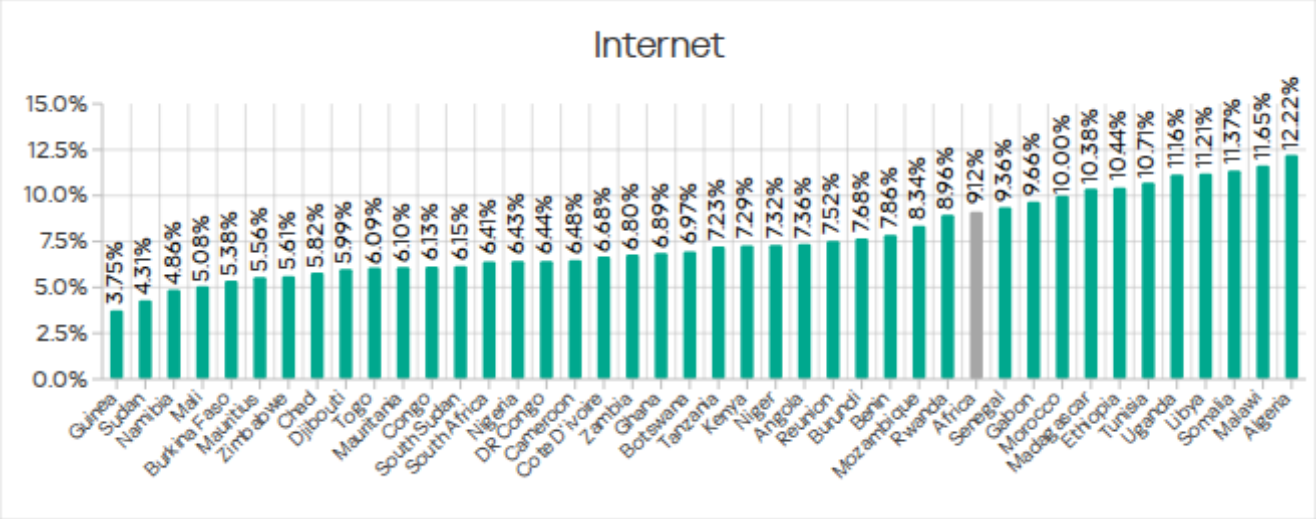
The rates for all threat sources, with the exception of network folders, decreased during the quarter. The percentage of ICS computers on which threats from network folders were blocked increased by 0.007 pp.



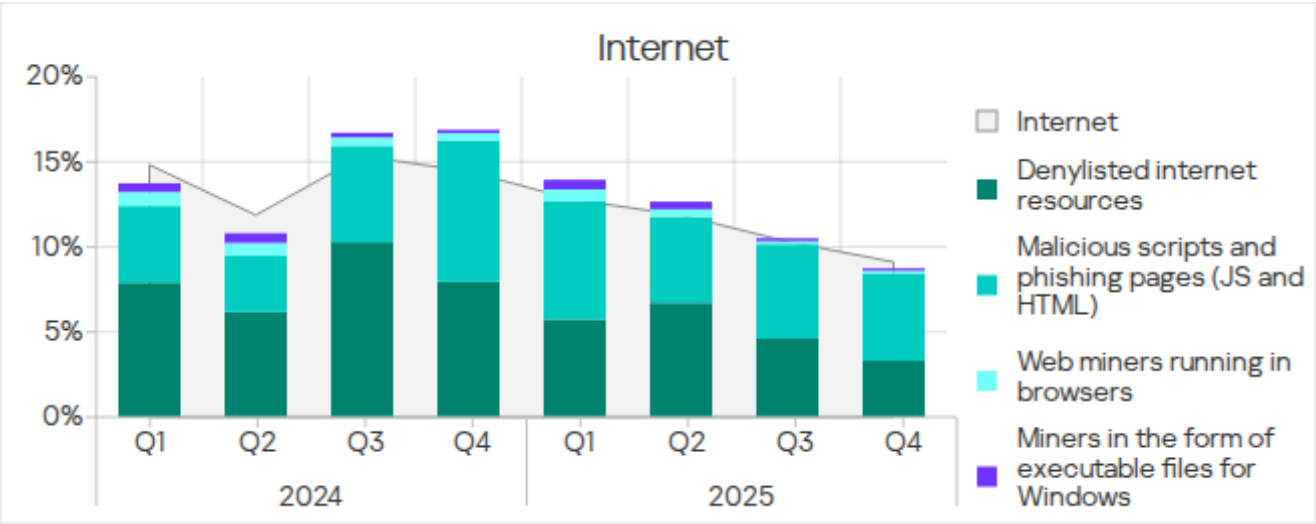
Internet

In Q4 2025, Africa dropped from first to third place globally in terms of the percentage of ICS computers on which internet threats were blocked. This is the third time in three years that a region has relinquished the top spot in this ranking. With a rate of 9.12%, Africa surpassed Northern Europe (the lowest ranking region) by a factor of 2.3.

Algeria leads the region with 12.22%. By contrast, Guinea had a much smaller percentage of ICS computers with blocked internet threats (3.75%).



The primary internet threat categories blocked on ICS computers in Q4 2025 were malicious scripts and phishing pages, denylisted internet resources, and malicious documents.

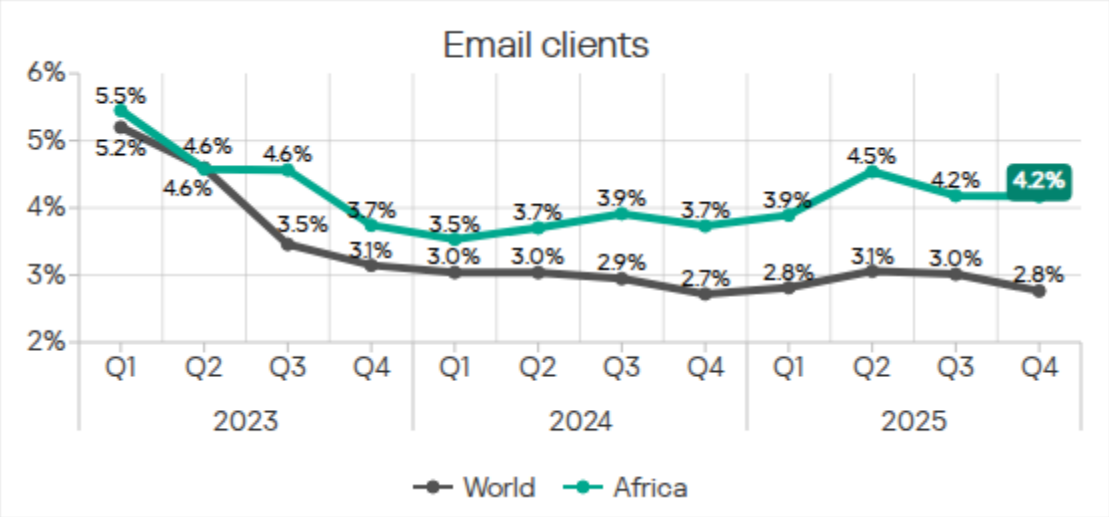


Email clients

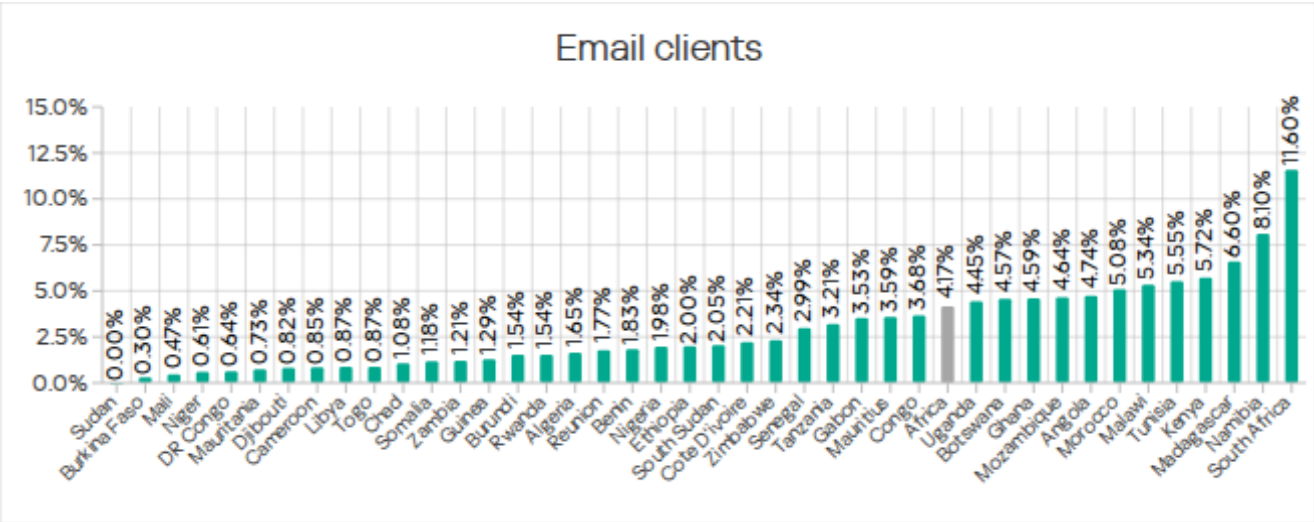
Africa still ranks fifth by percentage of ICS computers on which email client threats were blocked.

After increasing during the first two quarters of 2025, the figure decreased. Despite declining in the second half of the year, the quarterly figures for 2025 were higher than in the previous five quarters.

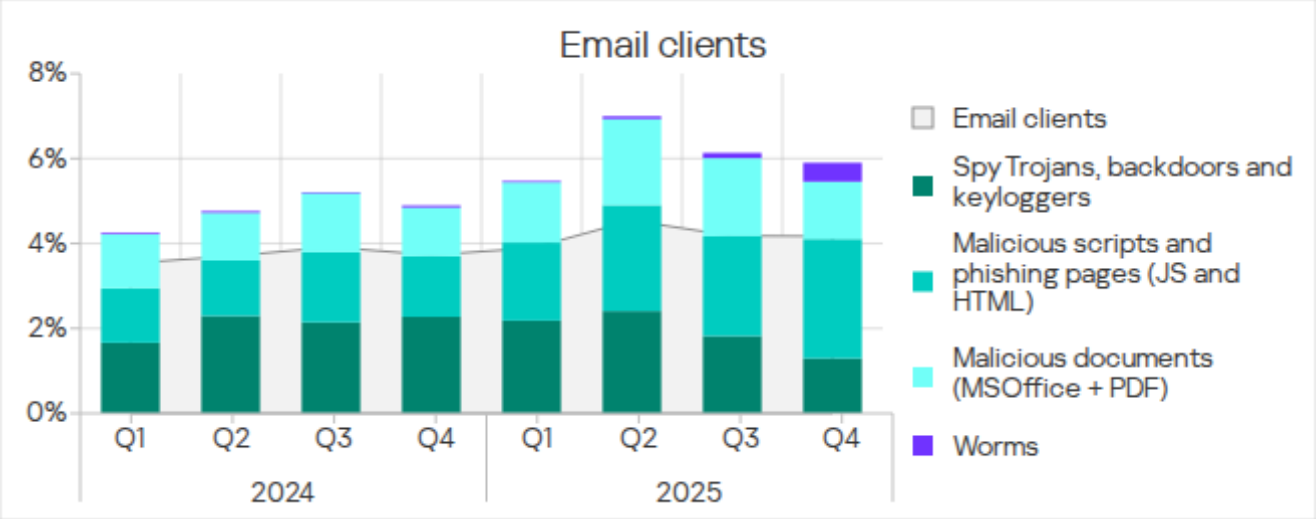
In Q4 2025, the percentage of ICS computers on which email client threats were blocked in Africa was 4.17%. This is 6.5 times higher than in Northern Europe, which ranked last.



South Africa had the highest percentage of ICS computers on which email client threats were blocked, with 11.60%. Burkina Faso had the lowest rate, at 0.3%.



The main email client threat categories blocked on ICS computers in Q4 2025 were malicious scripts and phishing pages, malicious documents, spyware, and worms.

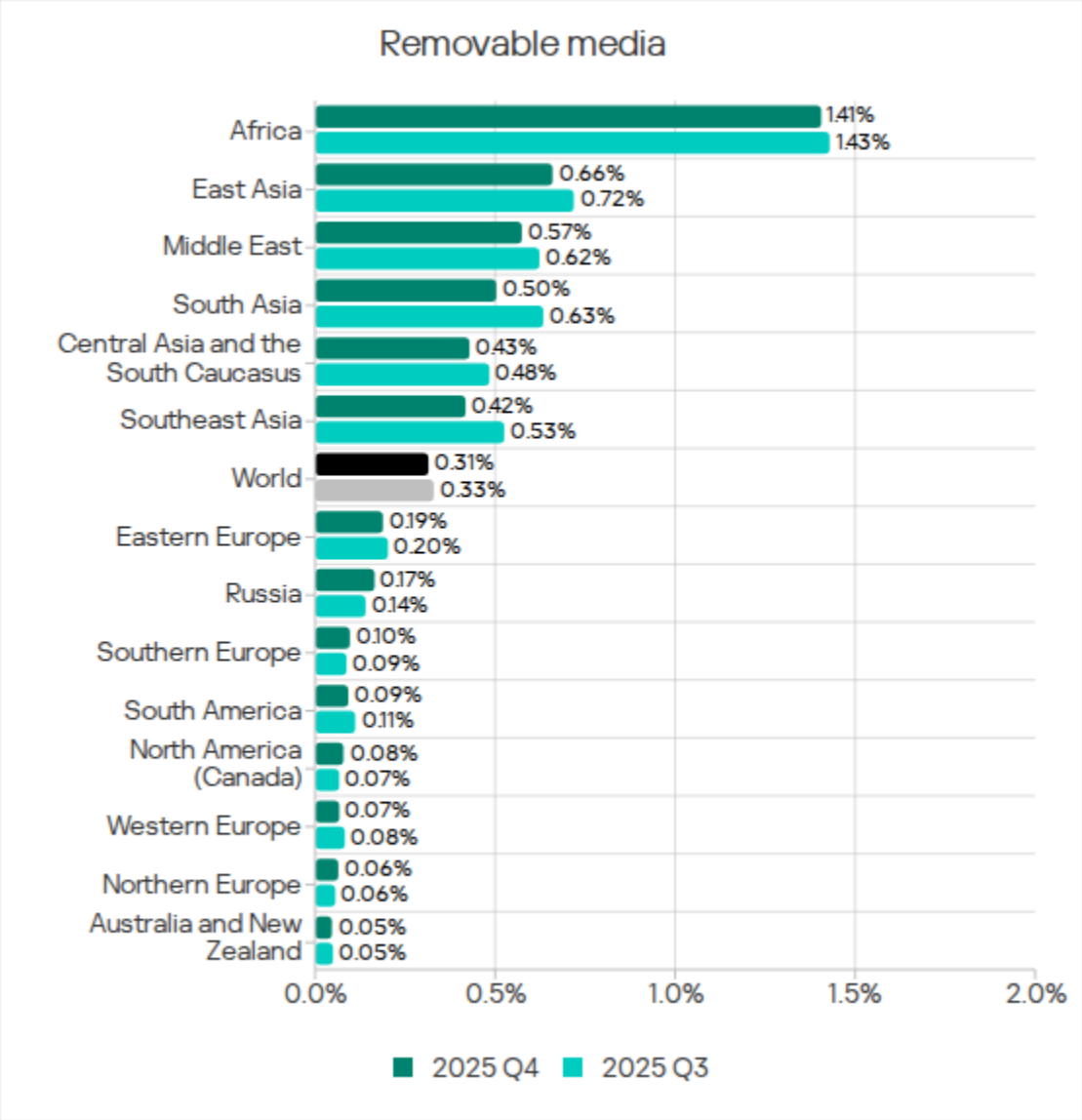


In Q4 2025, the percentage of worms originating from email clients increased significantly. This was due to a fresh wave of phishing attacks, known as Curriculum-vitae-catalina, in which phishing emails containing a malicious attachment (Backdoor.MSIL.XWorm) disguised as a resume were sent to victims. The attack peaked in Africa in November.

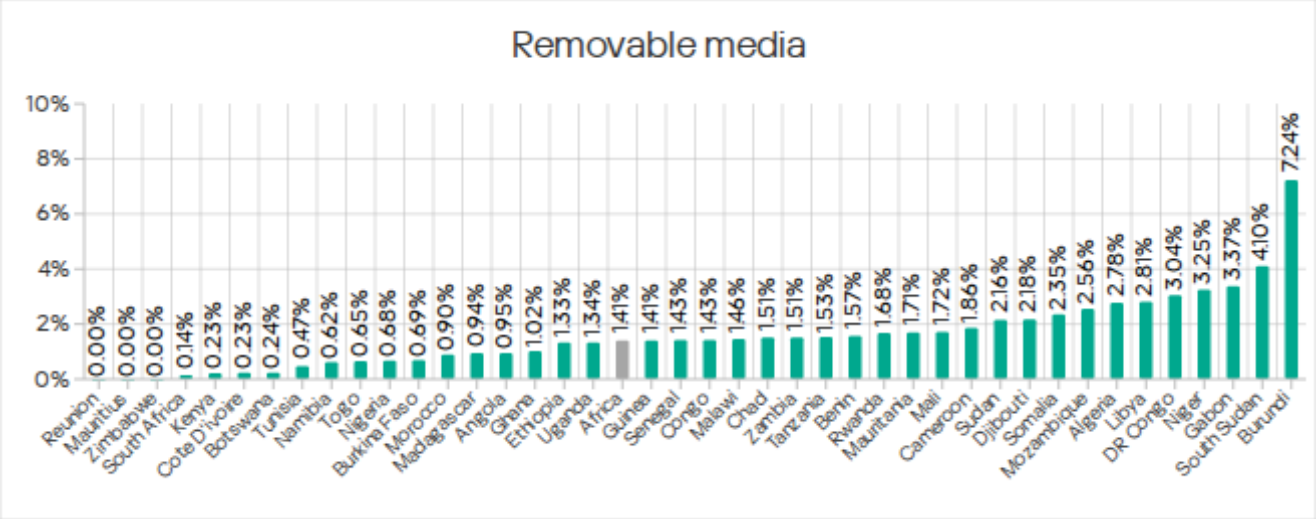
Although email was the main channel for distributing the malware, the threat was also detected in Africa when removable devices were connected to ICS computers because USB storage media is still actively used there.

Removable media

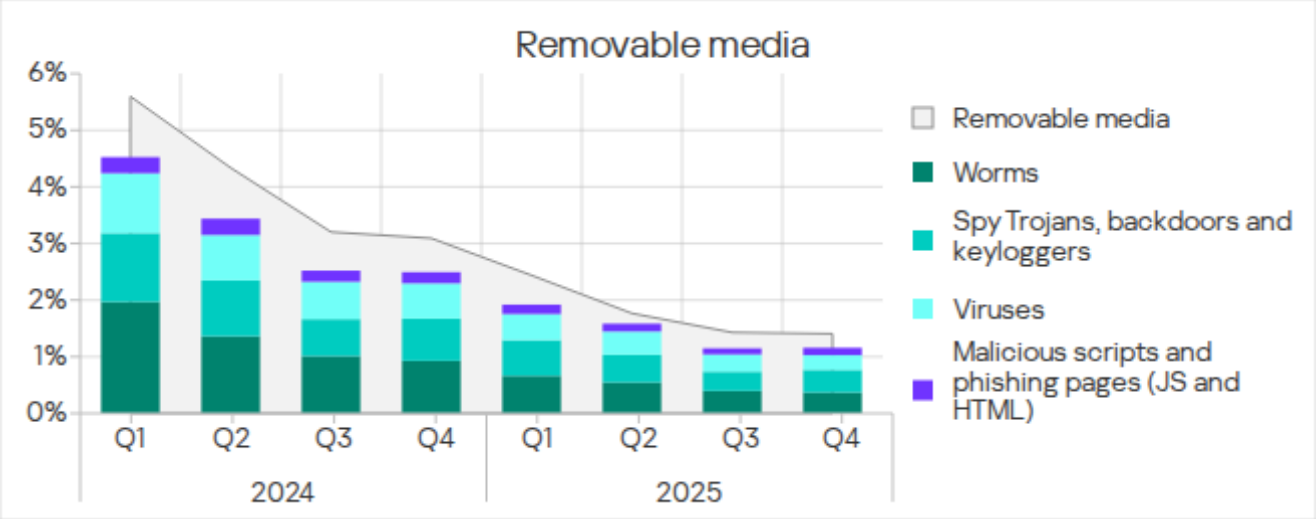
Despite a steady decline in the percentage of ICS computers on which removable media threats were blocked, Africa continued to lead the world by a large margin based on this indicator. Africa's figure of 1.41% was 28.2 times higher than that of Australia and New Zealand, the region with the lowest rate.



Of all the countries in the region, Burundi had a significantly higher percentage of ICS computers on which threats were blocked when removable media was connected: 7.24%. The figures for the other countries ranged from 0.14% in South Africa to 3.37% in Gabon.

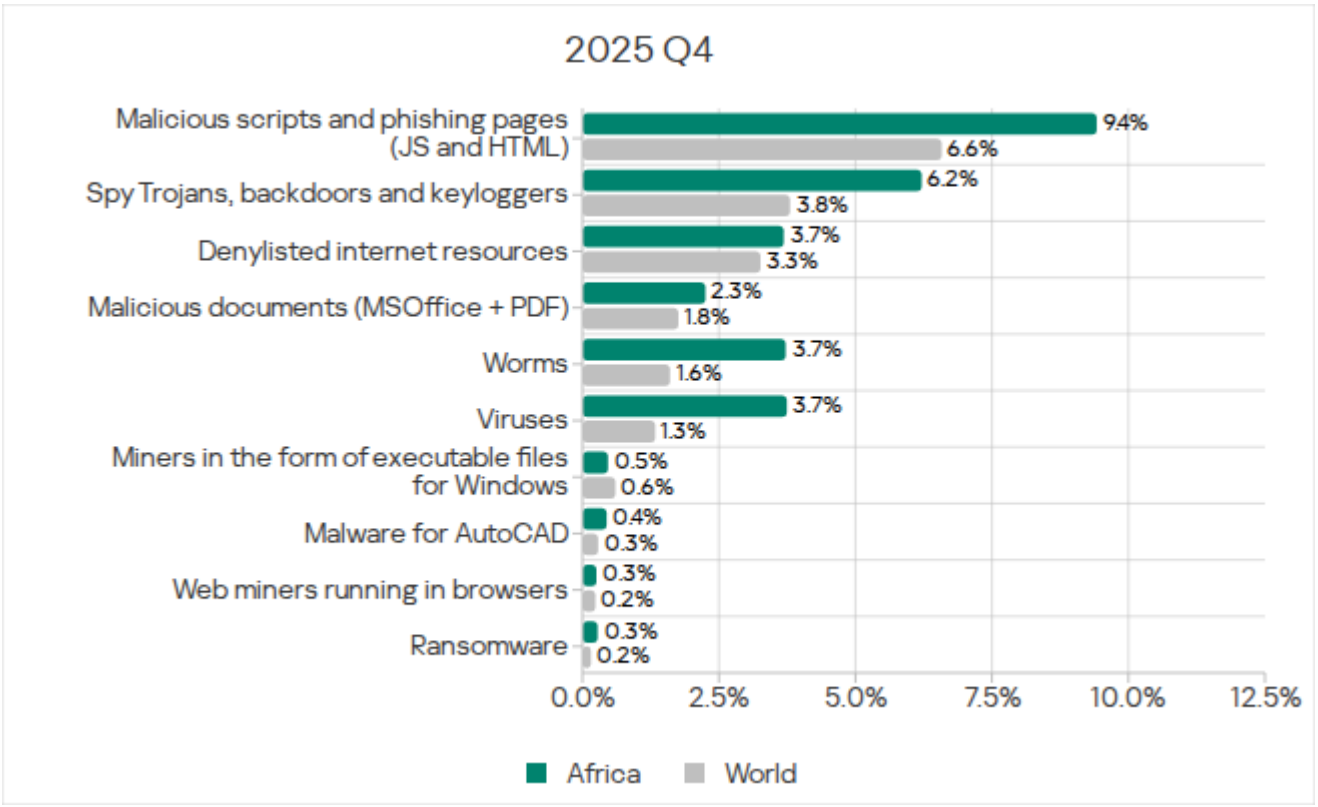


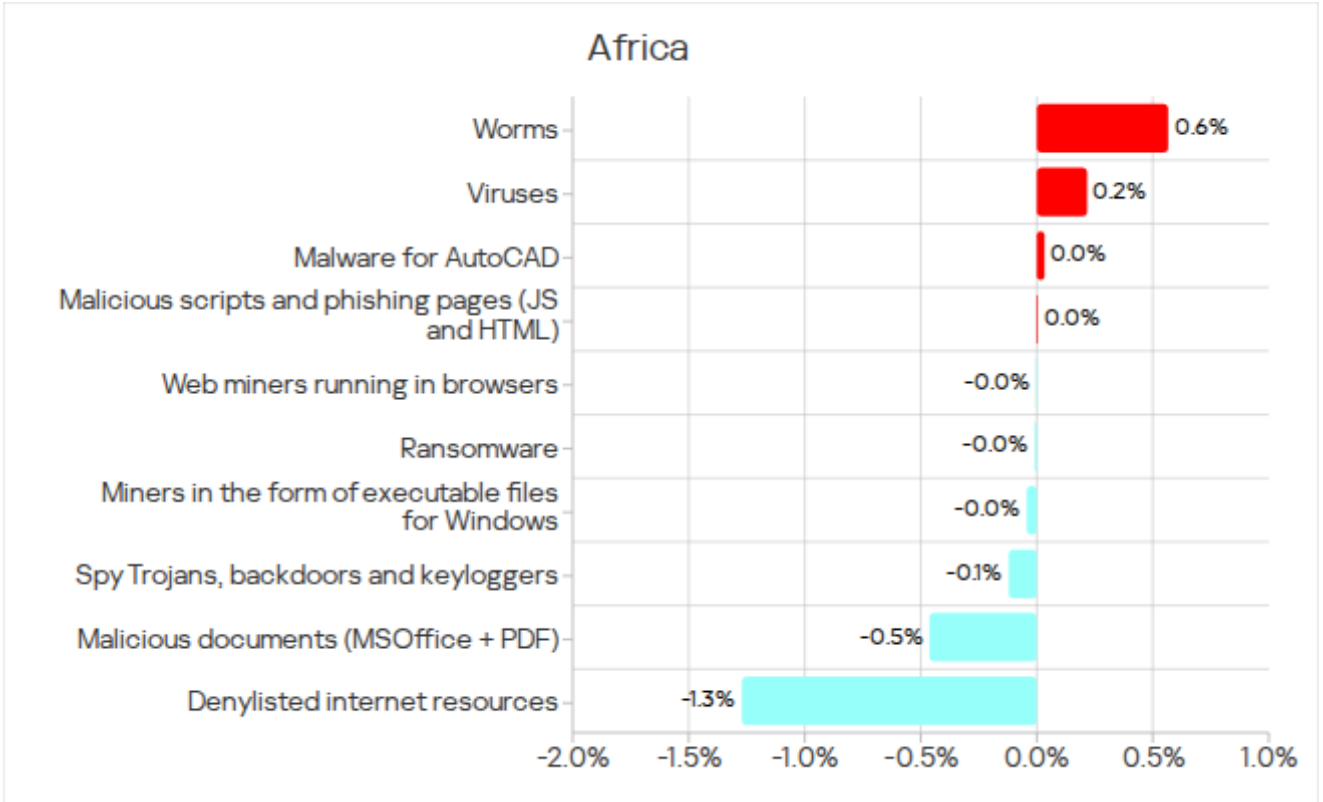
The main threat categories blocked on ICS computers from removable media in Q4 2025 were spyware, worms, and viruses. Africa also led the world in terms of the percentage of ICS computers on which spyware, and worms were blocked (it ranked second for viruses).



Threat categories

In Africa, the percentage of ICS computers on which malicious objects were blocked exceeded the global average in every threat category except miners in the form of executable files for Windows.





The most significant differences with global averages were seen in the following categories:

- Viruses: Africa's rate is 2.8 times higher
- Worms: 2.3 times higher
- Ransomware: 1.8 times higher
- Spyware: 1.6 times higher

In Q4 2025, Africa led the rankings in the percentage of ICS computers on which spyware and worms were blocked. The region ranked second in terms of viruses, as well as ransomware.

There was an increase in the figures for self-propagating malware (worms and viruses), malware for AutoCAD, and a slight increase for malicious scripts and phishing pages.

In terms of the percentage of ICS computers on which denylisted internet resources were blocked, Africa fell from first to second place. In Q4 2025, this indicator continued to decrease in all regions, with Africa also ranking second in terms of decline.

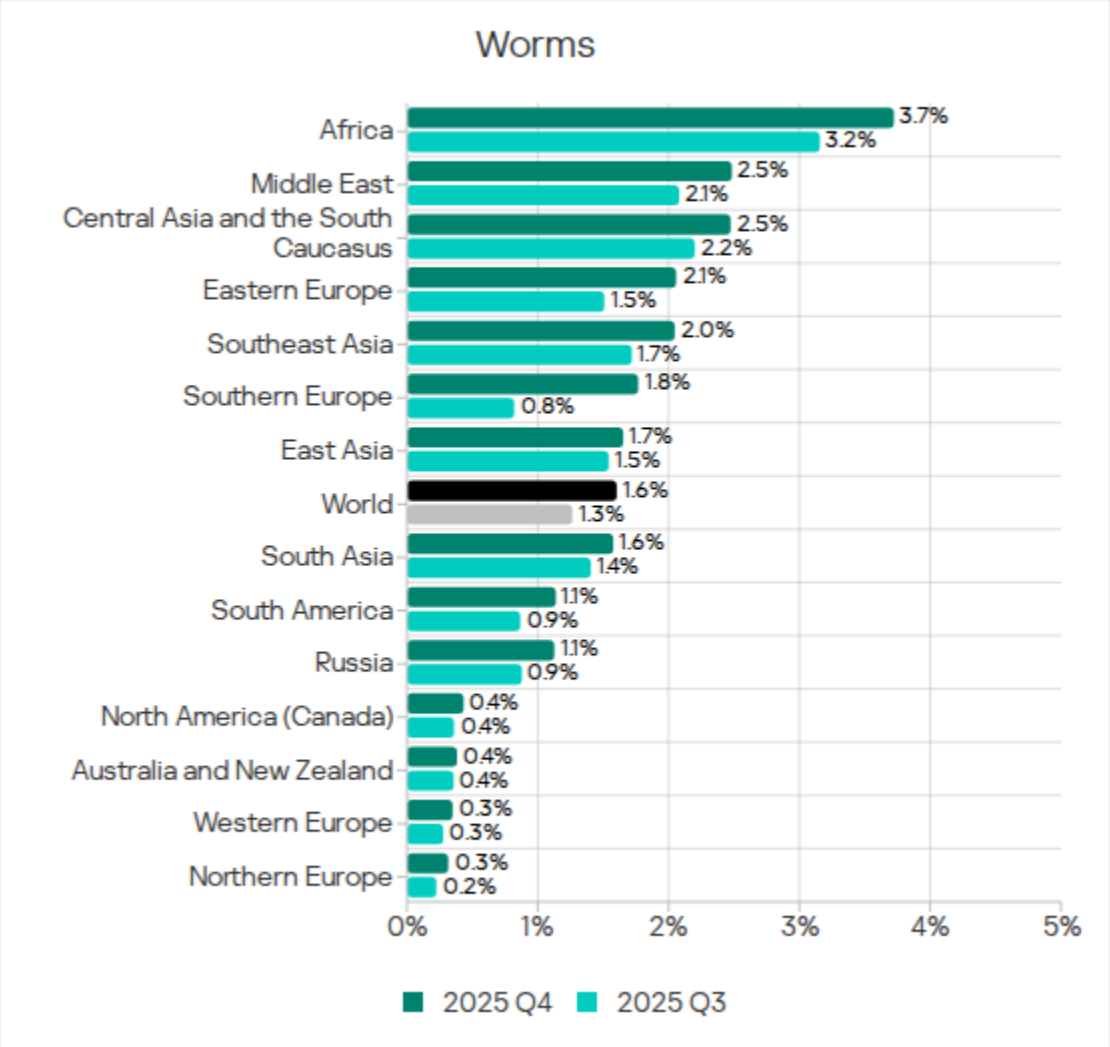
Self-propagating malware: worms and viruses

Worms and viruses are the main threat categories blocked when connecting removable media to ICS computers. Given Africa's consistent top ranking for this threat source, it's unsurprising that worms and viruses spread faster there than in other regions.

Worm rates were higher than those of viruses in 2022–2023, but since Q4 2024, the percentage of ICS computers on which viruses were blocked has been slightly higher.

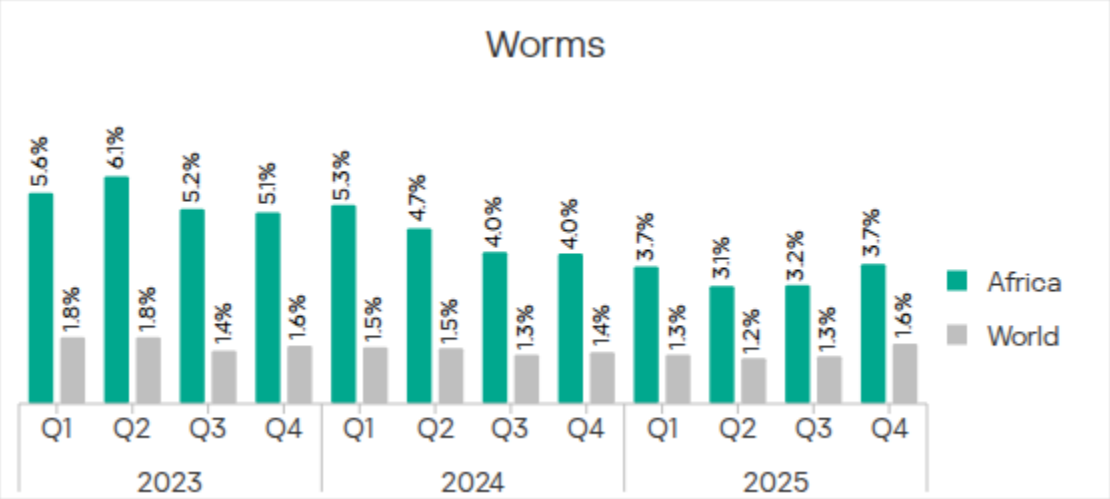
Worms

Africa remains the region with the highest percentage of ICS computers on which worms are blocked. As with the threat rate for removable media, the worm rate is gradually decreasing. Despite this, it is still significantly higher than in other regions.

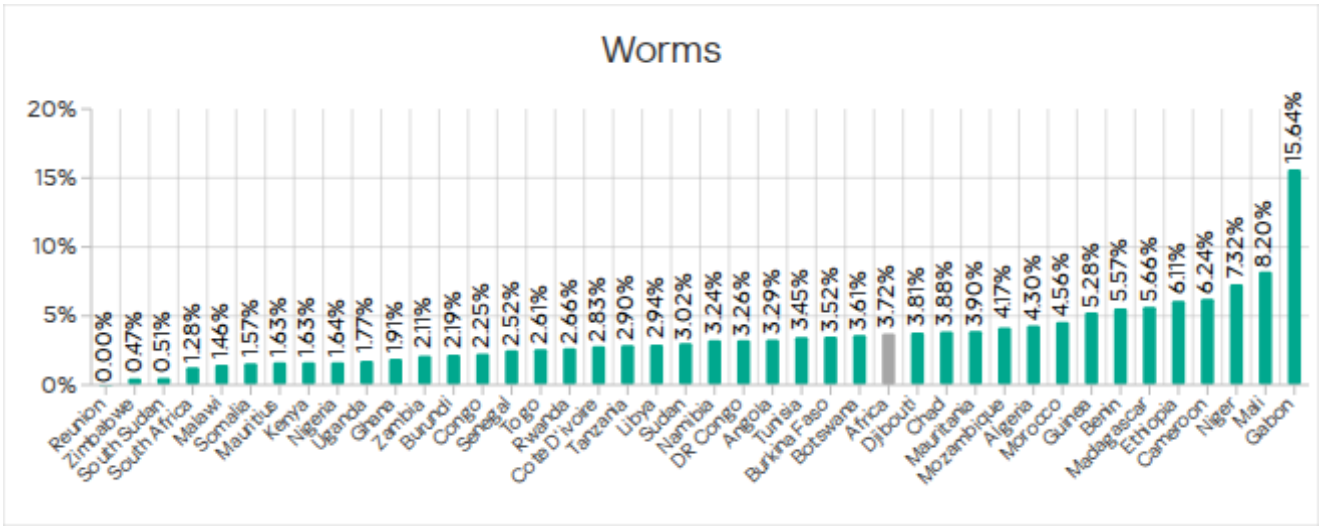


In Q4 2025, the percentage of ICS computers on which worms were blocked in Africa increased to 3.72%. This is 11.6 times higher than the rate in Northern Europe, which ranked last.

It should be noted that the worm rate increased in all regions due to a rise in phishing attacks aimed at delivering the Backdoor.MSIL.XWorm malware. In terms of the percentage increase in the number of ICS computers on which worms were blocked, Africa ranked second among all the regions.



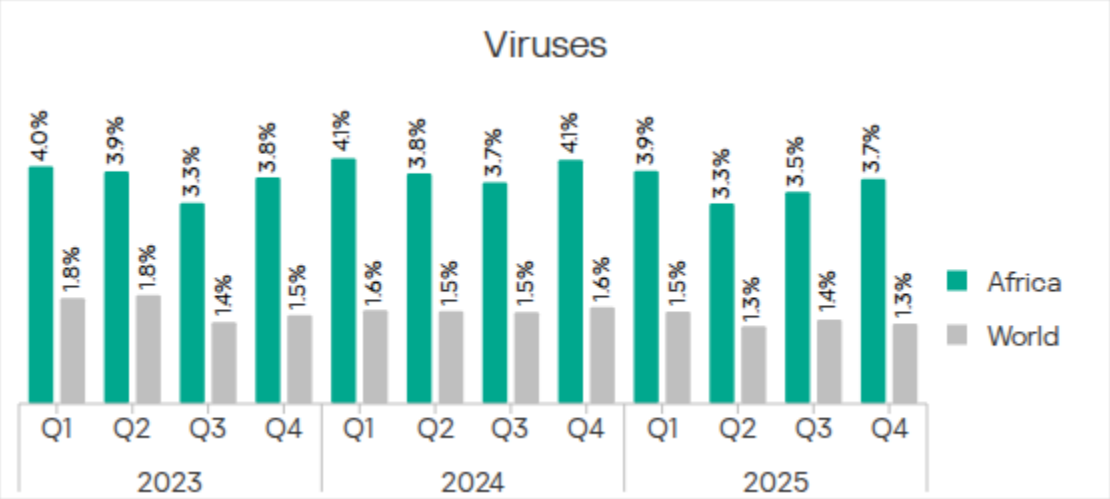
Among the countries in the region, Gabon led with an anomalously high figure of 15.64%. This was 1.9 times higher than the next country, Mali (8.20%). The lowest figure was in Zimbabwe at 0.47%.



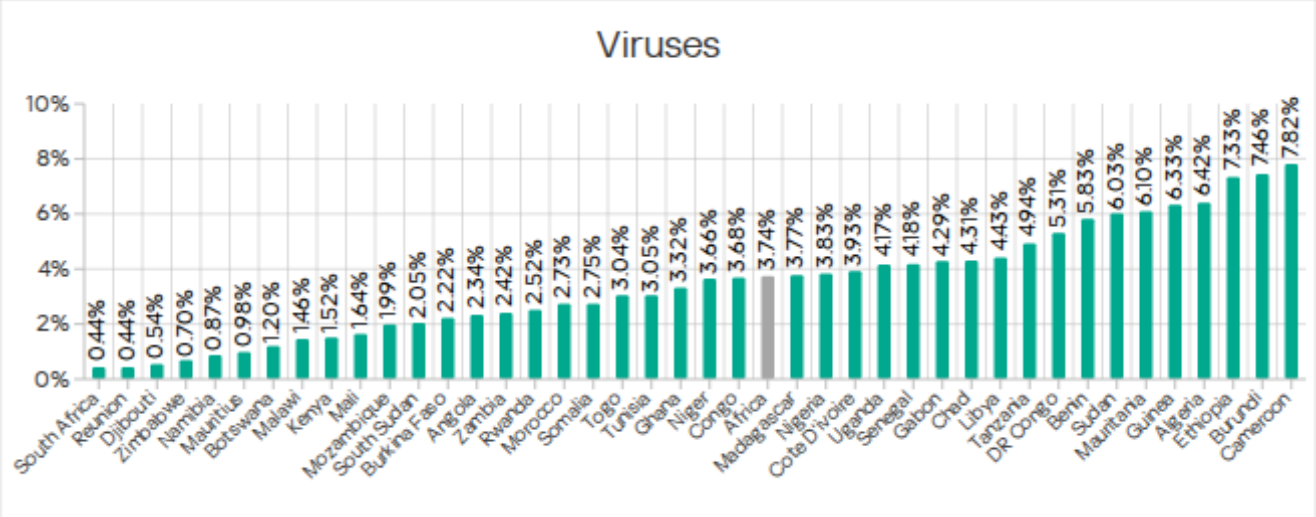
Viruses

In terms of the percentage of ICS computers on which viruses were blocked, Africa ranked second globally with 3.74%. This was 24.9 times higher than Western Europe, which came last.

In Q4 2025, Africa's rate increased and the region ranked first in terms of growth.

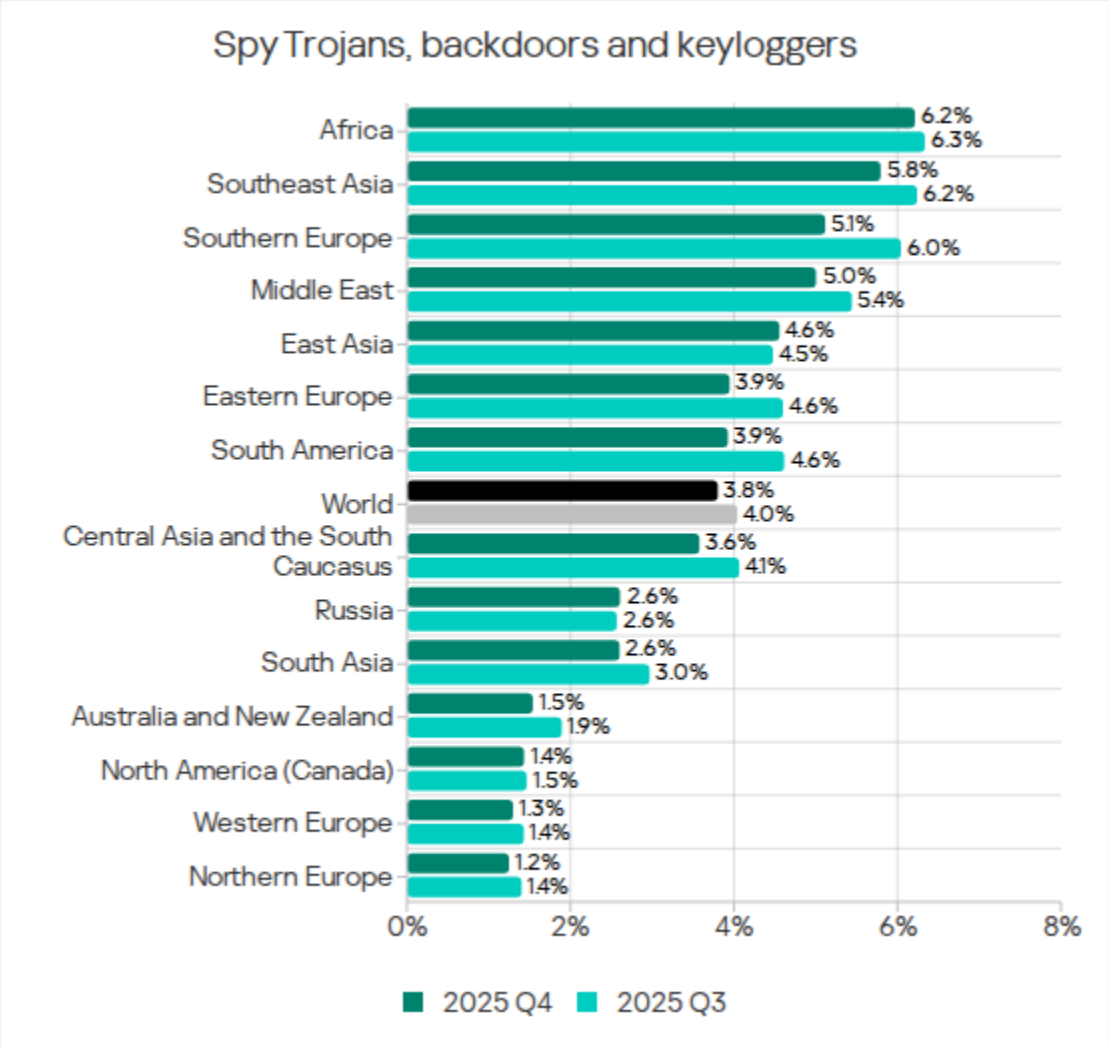


Cameroon (7.82%) led the region by percentage of ICS computers on which viruses were blocked. South Africa had the lowest figure (0.44%).

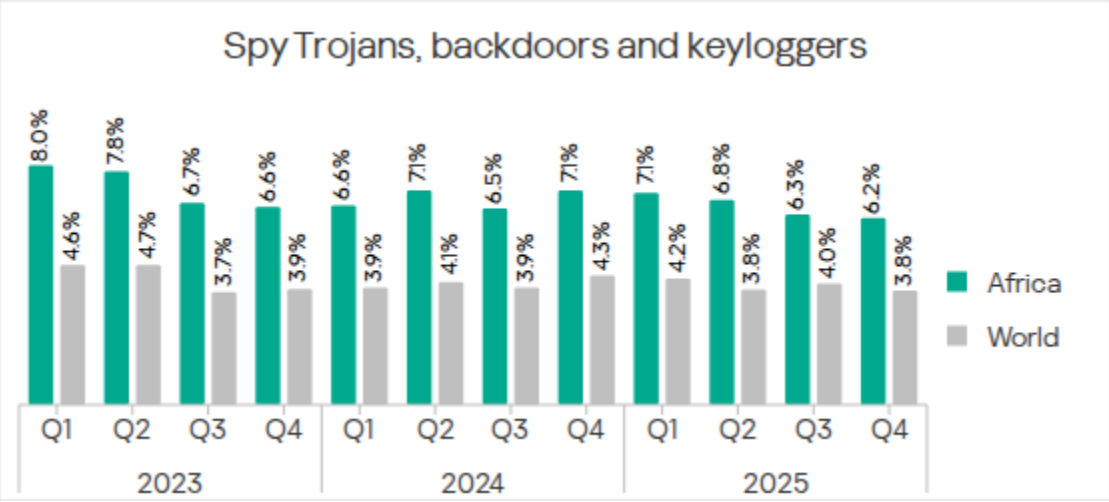


Spyware

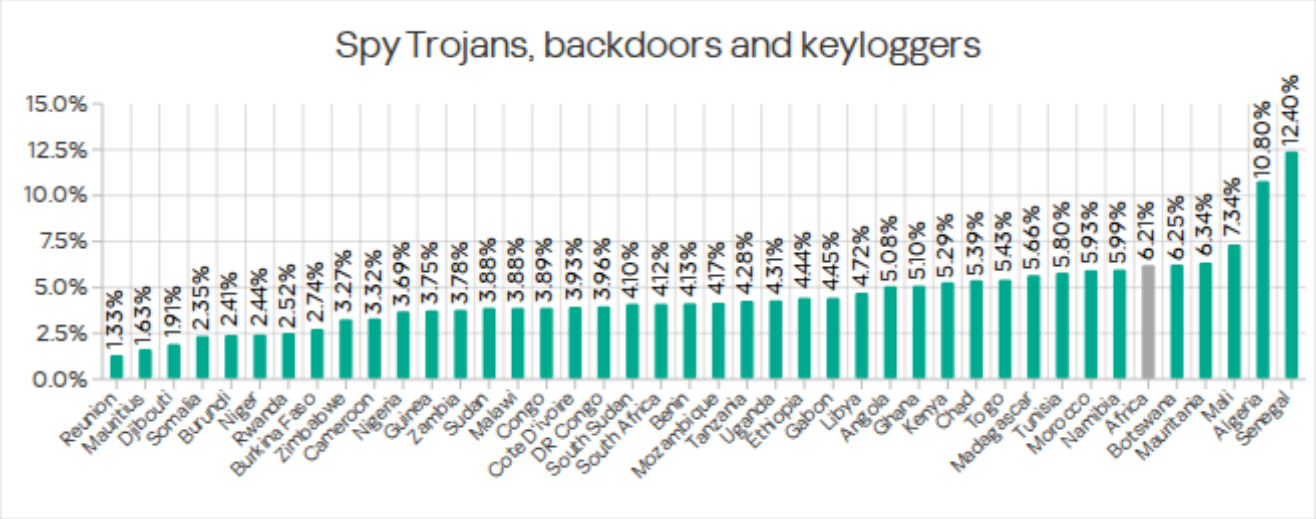
Africa consistently leads the regions in terms of the percentage of ICS computers on which spyware is blocked.



This indicator has been declining in the region for the last four consecutive quarters. In Q4 2025, it decreased to 6.21%. This was 5.0 times higher than in Northern Europe, which had the lowest figure.



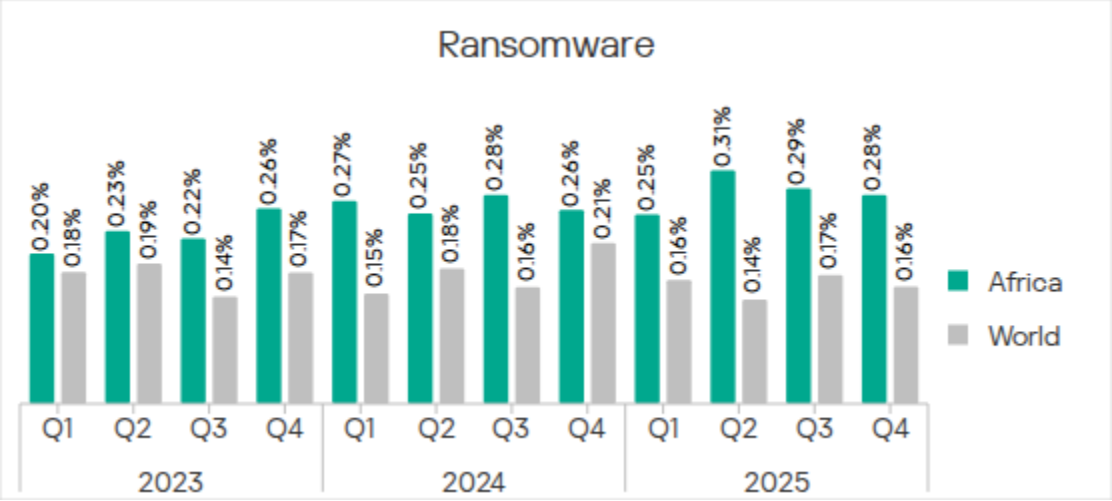
Senegal and Algeria led the region by a wide margin in terms of the percentage of ICS computers on which spyware was blocked, with 12.40% and 10.80%, respectively. Mauritius had the lowest rate (1.63%).



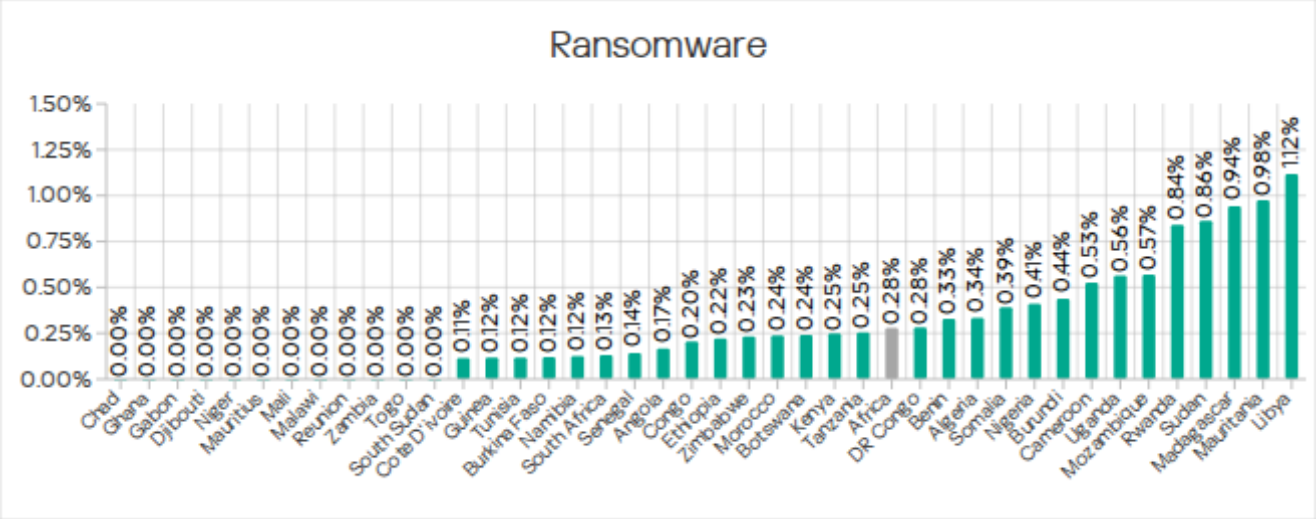
Ransomware

In Q4 2025, Africa ranked second globally in terms of the percentage of ICS computers on which ransomware was blocked, with 0.28%. This figure is 5.6 times higher than that of Northern Europe, which had the lowest rate.

The figure has decreased in the region for two consecutive quarters.



Libya had the highest percentage of ICS computers on which ransomware was blocked in the region, at 1.12%.

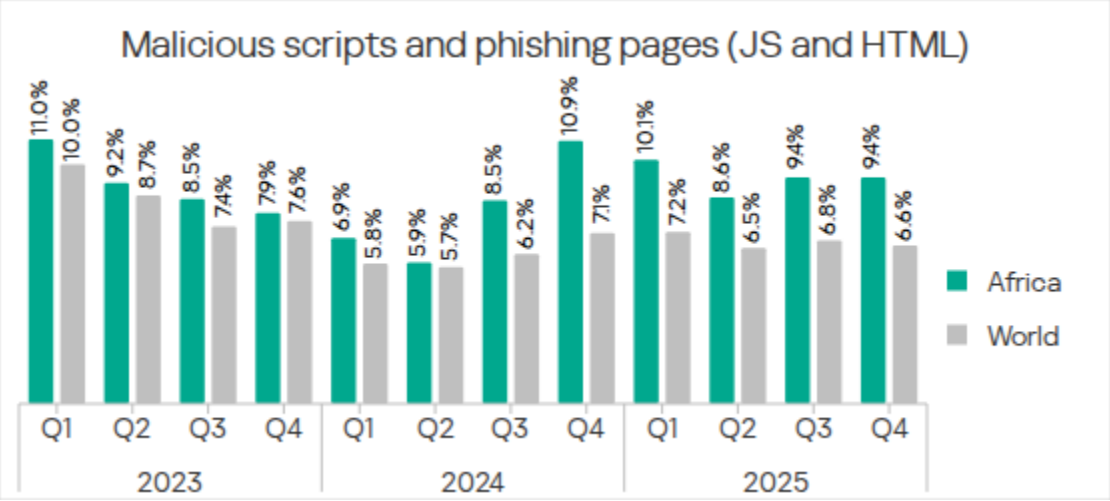


Notably, this threat was not detected in every country in the region in Q4 2025.

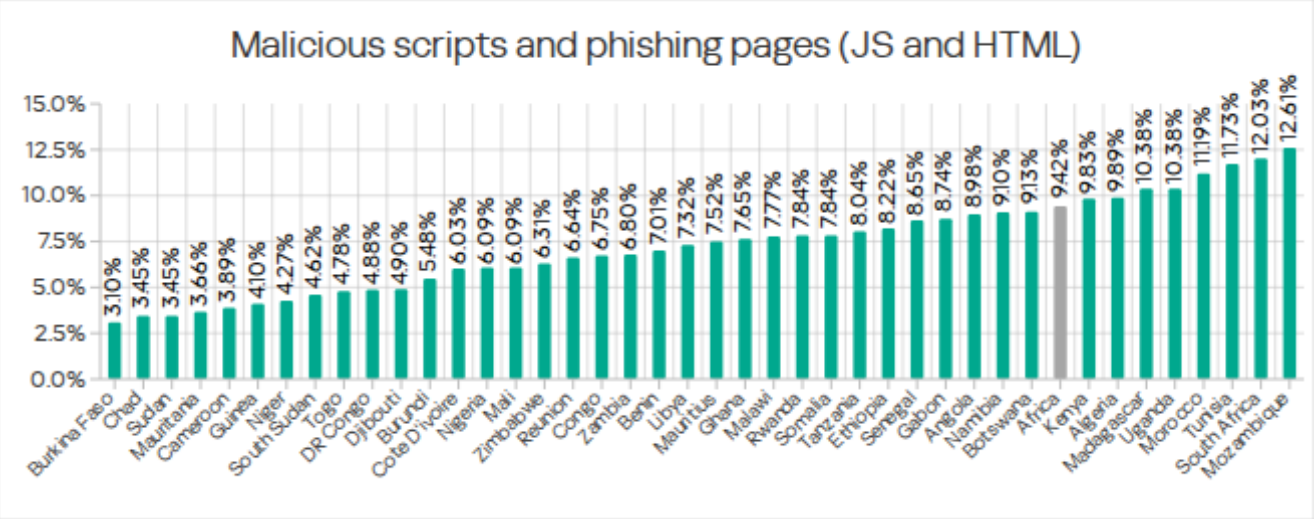
Malicious scripts and phishing pages

In Q3 2025, Africa rose from fourth to first place globally based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked. In Q4, the figure increased from 9.41% to 9.42%, but Africa dropped to third place in this ranking.

Africa's rate was 1.4 times higher than the global average and 3.7 times higher than that of Northern Europe, which ranked last.

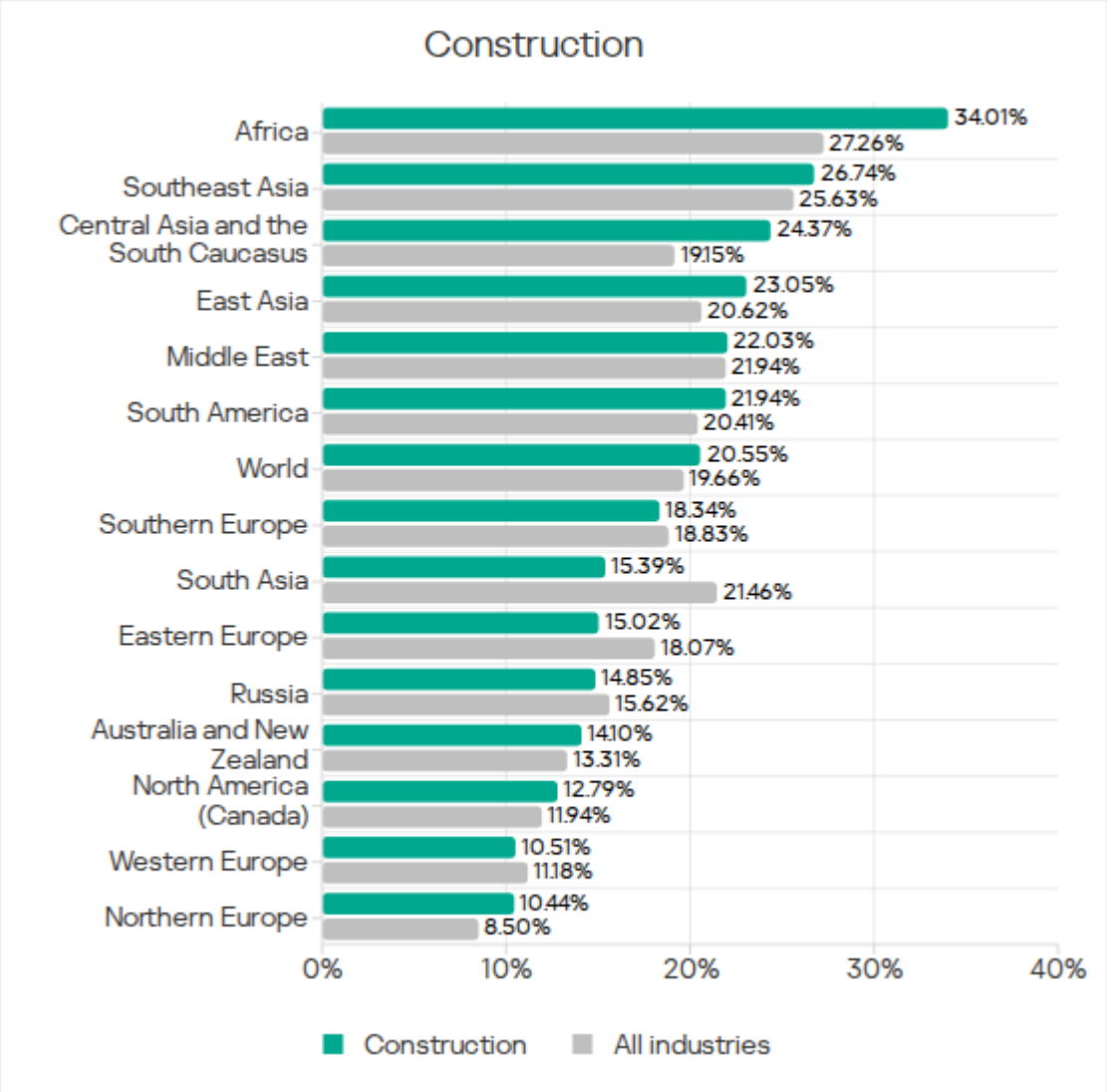


Mozambique had the highest percentage of ICS computers on which malicious scripts and phishing pages were blocked, at 12.61%. Burkina Faso had the lowest figure, at 3.10%.

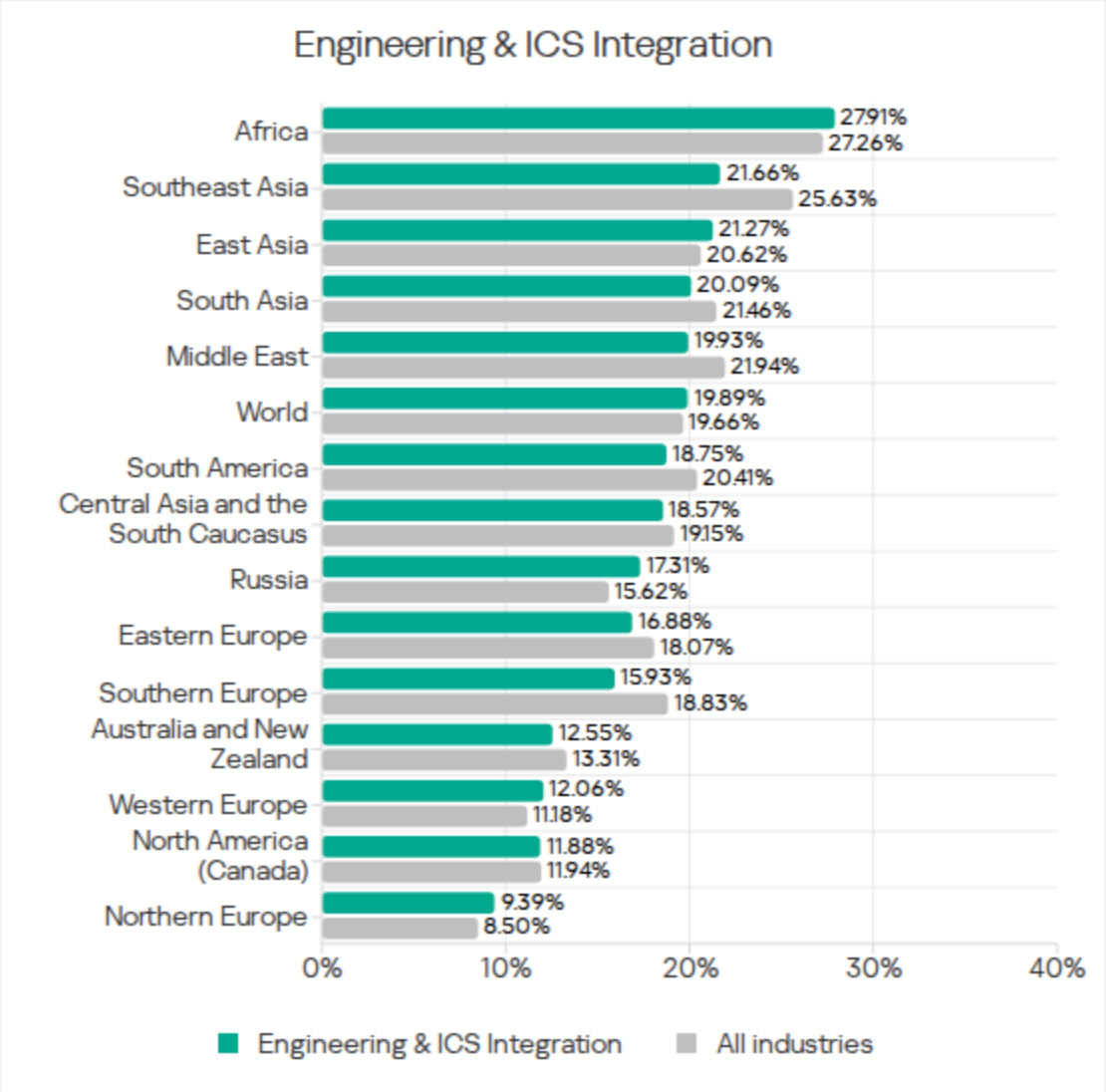


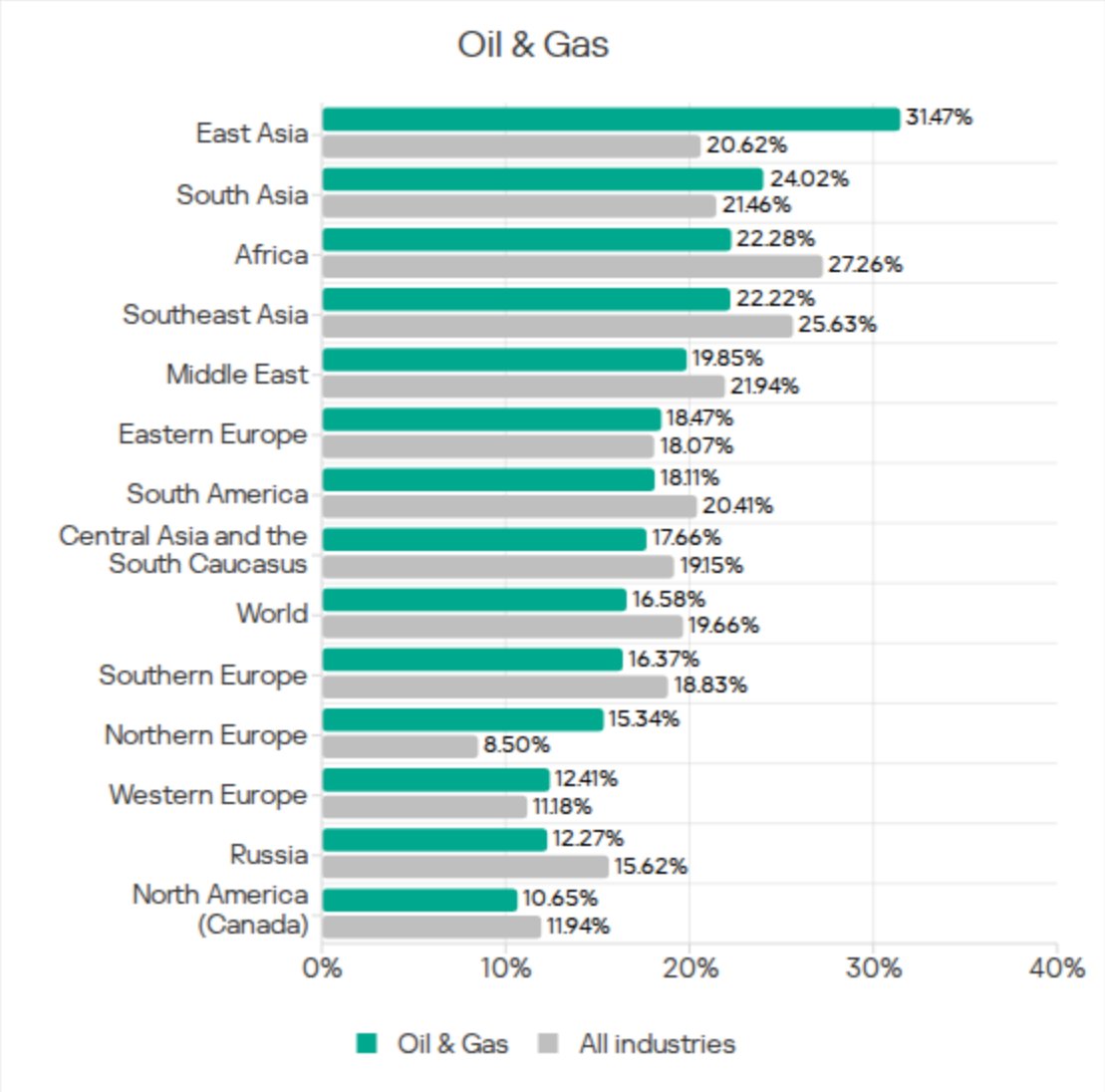
Industries

In Africa, construction remains the most frequently threatened industry among those covered in this report. Africa leads globally in the percentage of ICS computers on which malicious objects were blocked in this industry.

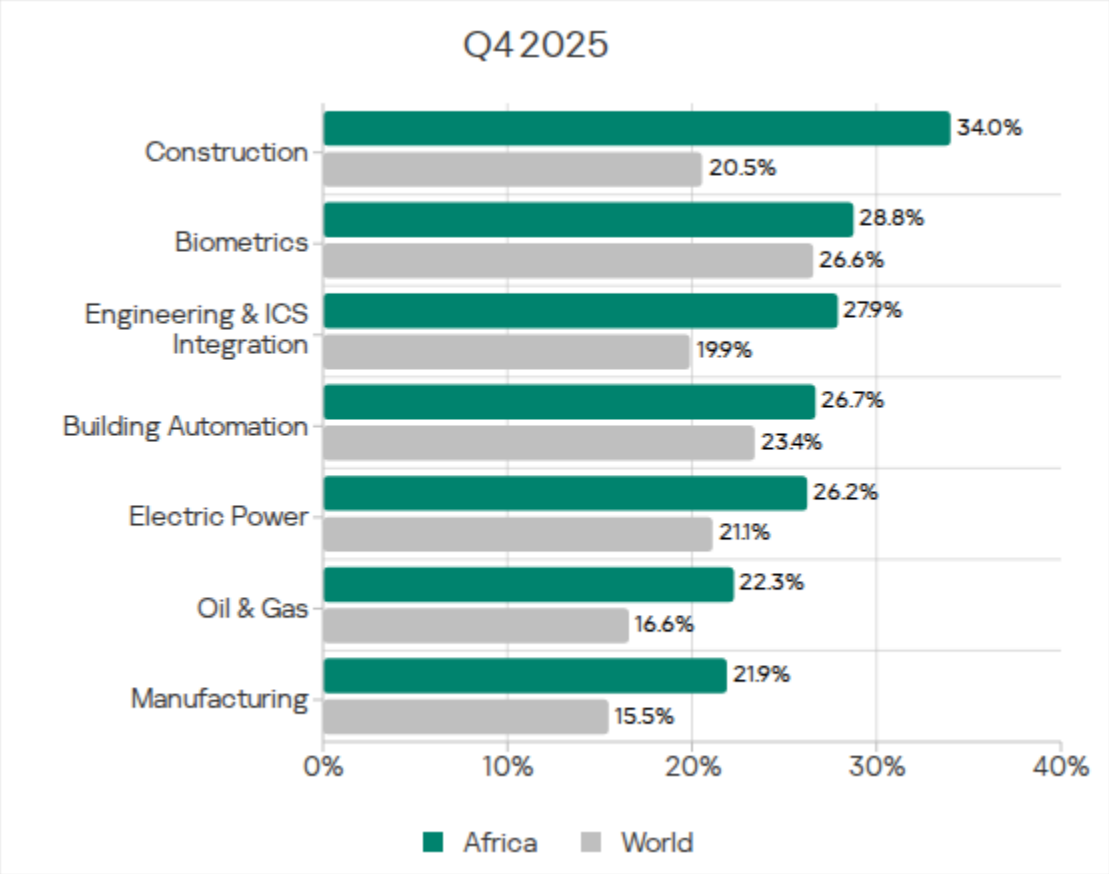


Africa also led in the engineering and ICS integrators, and oil and gas industries.

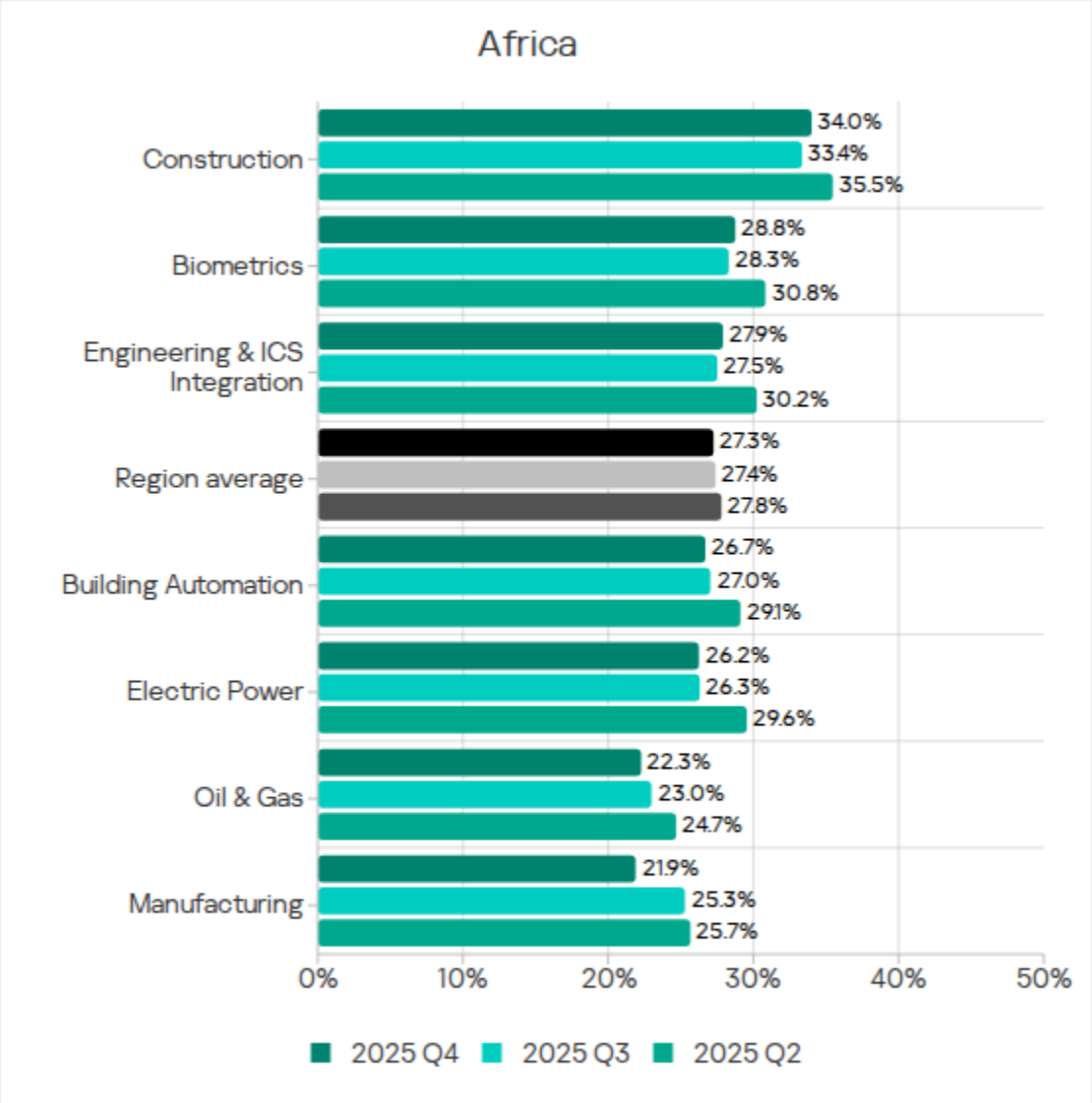




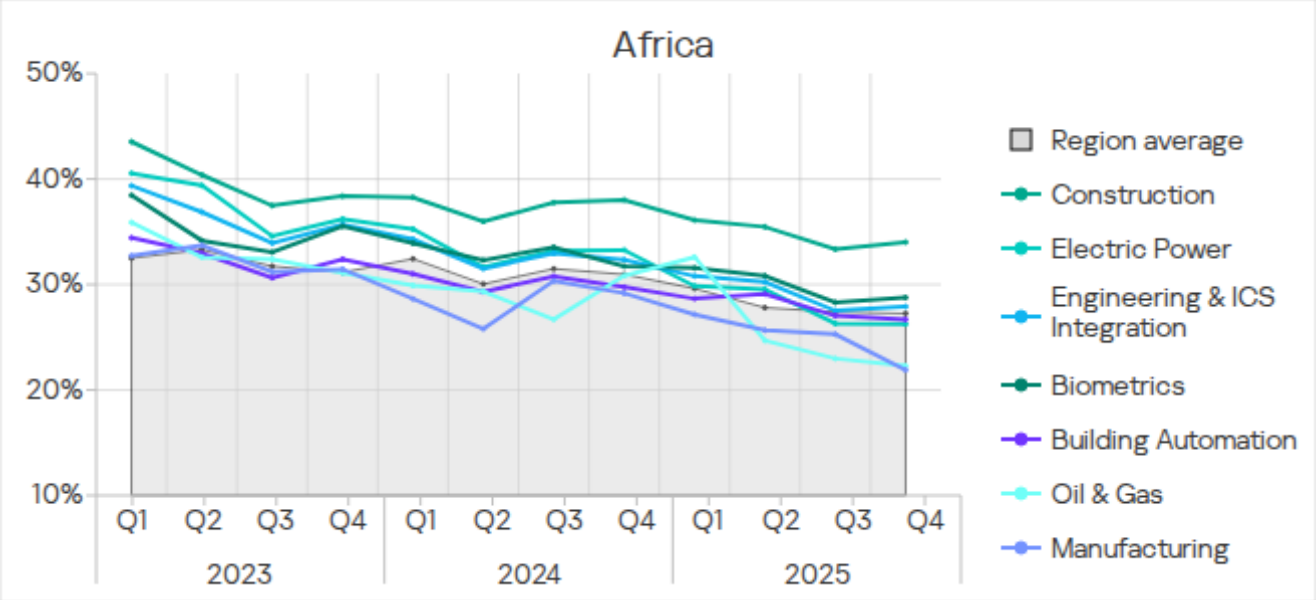
All the region's industries exceed the respective global averages. The largest differences were in construction (1.6 times), manufacturing, and oil and gas (both 1.5 times).



In Q4 2025, increases were seen in three industries: construction, biometrics, and engineering and ICS integrators.



All the industries covered show positive long-term trends (decreasing values) with significant periodic fluctuations.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in Africa, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	9.18%	8.47%	11.00%	9.65%	8.56%	12.02%	8.83%	9.12%
Email clients	6.00%	7.12%	2.65%	2.37%	0.29%	3.35%	3.06%	4.17%
Removable media	1.49%	1.00%	1.53%	1.79%	1.36%	1.34%	0.36%	1.41%
Network folders	0.10%	0.03%	0.02%	0.03%	—	0.03%	—	0.03%
Industry metric in region	28.76%	26.69%	27.91%	26.25%	22.28%	34.01%	21.89%	

Threat category indicators for industries in Africa, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	3.25%	3.11%	4.52%	4.41%	4.18%	4.93%	3.96%	3.69%
Malicious scripts and phishing pages (JS and HTML)	11.00%	11.46%	9.54%	8.06%	6.61%	10.34%	7.75%	9.42%
Malicious documents (MSOffice + PDF)	3.36%	3.60%	1.63%	1.81%	0.68%	2.16%	1.35%	2.25%
Spy Trojans, backdoors and keyloggers	8.10%	6.25%	5.97%	6.28%	5.64%	9.31%	3.60%	6.21%
Ransomware	0.35%	0.31%	0.29%	0.42%	0.49%	0.43%	0.27%	0.28%
Miners in the form of executable files for Windows	0.66%	0.44%	0.61%	0.47%	0.29%	0.88%	0.36%	0.47%
Web miners running in browsers	0.45%	0.29%	0.25%	0.22%	0.10%	0.33%	0.18%	0.26%
Malware for AutoCAD	0.18%	0.13%	0.34%	0.39%	0.88%	2.43%	0.18%	0.44%
Worms	4.74%	3.65%	3.50%	3.82%	3.31%	3.50%	2.79%	3.72%
Viruses	3.91%	2.93%	3.77%	4.30%	3.79%	6.60%	2.88%	3.74%
Industry metric in region	28.76%	26.69%	27.91%	26.25%	22.28%	34.01%	21.89%	

Construction

Africa ranked first among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the construction sector.

Among all industries across all regions, Africa's construction sector ranked:

- Second by percentage of computers where worms were blocked.

Across all regions, Africa ranked:

- First by percentage of ICS computers on which threats from removable media were blocked, and second for internet threats.
- First by percentage of ICS computers on which threats in the following categories were blocked: malicious scripts and phishing pages, spyware, ransomware, worms.
- Second for denylisted internet resources, ransomware, and viruses.
- Third in terms of malware for AutoCAD.

In the regional cross-industry rankings, the construction sector ranked:

- First in terms of the percentage of ICS computers on which threats from the internet were blocked, and third for both threats from email clients and network folders.
- First in multiple categories: denylisted internet resources, spyware, viruses, malware for AutoCAD, and miners in the form of executable files for Windows.
- Second in terms of web miners, and ransomware.
- Third for malicious scripts and phishing pages, and malicious documents.

Biometrics

Africa ranked second among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the biometrics.

Among all industries and across all regions, Africa's biometrics ranked:

- Third in the percentage of ICS computers on which worms were blocked.

Across all regions, Africa ranked:

- First in the percentage of ICS computers on which threats from removable media were blocked, and second both in terms of threats from the internet and network folders.
- First in the percentage of ICS computers on which viruses, and worms were blocked.
- Second for spyware.
- Third for denylisted internet resources.

Within Africa's industries, biometrics ranked:

- First in the percentage of ICS computers on which threats from network folders were blocked, second for threats from email clients, and third for threats from removable media.
- First in the percentage of ICS computers on which web miners and worms were blocked.

- Second in the following categories: malicious scripts and phishing pages, malicious documents, spyware, and miners in the form of executable files for Windows.
- Third in terms of viruses.

Engineering and ICS integrators

Africa ranked first among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators sector.

Across all regions, Africa ranked:

- First in the percentage of ICS computers on which threats from removable media were blocked, and second for threats from the internet.
- First in the percentage of ICS computers on which denylisted internet resources, spyware, ransomware, viruses, and worms were blocked.
- Second for malicious scripts and phishing pages.
- Third in terms of miners in the form of executable files for Windows.

In the regional cross-industry rankings, engineering and ICS integrators ranked as follows:

- Second in the percentage of ICS computers on which threats from the internet as well as removable media were blocked.
- Second in the percentage of ICS computers on which denylisted internet resources were blocked.
- Third in terms of miners in the form of executable files for Windows.

Building automation

Africa ranked second among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the building automation sector.

Across all regions, Africa ranked:

- First in the percentage of ICS computers on which threats from removable media were blocked.
- Second in the percentage of ICS computers on which viruses were blocked.
- Third place in terms of worms, and web miners.

In the regional cross-industry rankings, building automation ranked as follows:

- First in the percentage of ICS computers on which threats from email clients were blocked, and second for threats from network folders.
- First in the percentage of ICS computers on which malicious documents, as well as malicious scripts and phishing pages, were blocked.
- Third place in terms of worms, and web miners.

Electric power

Africa ranked second among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the electric power industry.

Across all regions, Africa ranked:

- Second in the percentage of ICS computers on which threats from internet and removable media were blocked.
- First in the percentage of ICS computers on which worms were blocked.
- Second for spyware and ransomware.
- Third in terms of malicious scripts and phishing pages, viruses, and malware for AutoCAD.

In the regional cross-industry rankings, the electric power industry ranked:

- First in the percentage of ICS computers on which threats from removable media were blocked, and third in terms of threats from the internet.
- Second in the percentage of ICS computers on which worms, and viruses were blocked.
- Third in the following categories: denylisted internet resources, spyware, ransomware, malware for AutoCAD.

Manufacturing

Africa ranked second among the regions in terms of the percentage of ICS computers on which malicious objects were blocked in the manufacturing sector.

Across all regions, Africa ranked:

- Second in the percentage of ICS computers on which threats from the internet and email clients were blocked.
- First in the percentage of ICS computers on which denylisted internet resources, and worms were blocked.
- Second for ransomware.
- Third in terms of malicious scripts and phishing pages, spyware, and viruses.

Oil and gas

Africa ranked first among regions in terms of the percentage of ICS computers on which malicious objects were blocked in the oil and gas industry.

Across all regions, Africa ranked:

- First in the percentage of ICS computers on which threats from removable media were blocked, and second in terms of threats from the internet.
- First in the percentage of ICS computers on which spyware, ransomware, viruses, and malware for AutoCAD were blocked.
- Second in terms of denylisted internet resources, and malicious scripts and phishing pages.

In the regional cross-industry rankings, the oil and gas industry ranked:

- First in the percentage of ICS computers on which ransomware was blocked.
- Second in terms of malware for AutoCAD.

Methodology used to prepare statistics

This report presents the results of analyzing statistics obtained with the help of Kaspersky Security Network (KSN). The data was received from KSN users who consented to its anonymous sharing and processing for the purposes described in the KSN Agreement for the Kaspersky product installed on their computer.

The benefits of joining KSN for our customers include faster response to previously unknown threats and a general improvement in the quality of detection by their Kaspersky installation achieved by connecting to a cloud-based repository of malware data that is not transferable to the customer in its entirety by nature of its size and the amount of resources that it uses.

Data shared by the user contains only the data types and categories described in the appropriate KSN Agreement. This data helps to a significant extent in analyzing the threat landscape and serves as a prerequisite for detecting new threats including targeted attacks and APTs[1].

Statistical data presented in the report was obtained from ICS computers that were protected with Kaspersky products and which Kaspersky ICS CERT categorized as enterprise OT infrastructure. This group includes Windows computers that serve one or several of the following purposes:

- Supervisory control and data acquisition (SCADA) servers
- Building automation servers
- Data storage (Historian) servers
- Data gateways (OPC)
- Stationary workstations of engineers and operators
- Mobile workstations of engineers and operators
- Human machine interface (HMI)
- Computers used to manage technological and building automation networks
- Computers of ICS/PLC programmers

Computers that share statistics with us belong to organizations from various industries. The most common are the chemical industry, metallurgy, ICS design and integration, oil and gas, energy, transport and logistics, the food industry, light industry, pharmaceuticals. This also includes systems from engineering and integration firms that work with enterprises in a variety of industries,

[1] We recommend that organizations subject to restrictions on sharing any data outside the corporate perimeter consider using Kaspersky Private Security Network.

as well as building management systems, physical security, and biometric data processing.

We consider a computer to have been attacked if a Kaspersky security solution blocked one or more threats on that computer during the review period: a month, six months, or a year depending on the context as can be seen in the charts above. To calculate the percentage of machines whose malware infection was prevented, we take the ratio of the number of computers attacked during the review period to the total number of computers in the selection from which we received anonymized information during the same period.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com