1. NATIONAL AND EA CYBER LANDSCAPE AND EXPOSURE PART 1

The cyber threat landscape in East Africa, particularly in Uganda, is becoming a prime target for malicious groups. As businesses increasingly rely on digital platforms to meet customer demands, they expose themselves to a growing number of cyberattacks. Critical assets such as product designs, distribution networks, customer data, and intellectual property are now at heightened risk, especially due to the extensive involvement of third parties throughout the value chain. This interconnectedness expands the attack surface, making it easier for cybercriminals to exploit vulnerabilities.

With an increasingly complex digital ecosystem across the region, millions of users, countless applications, and a variety of devices are interconnected, multiplying potential entry points for attackers. For financial institutions, fintech companies, online vendors, e-government initiatives with publicly accessible services, and other players in the payments and finance space, this presents serious risks. For example, payment gateways, customer account details, and transaction data are often targeted, exposing sensitive financial information. The risk is even higher when these entities engage with third-party service providers, such as cloud services or payment processors, which may not always have robust security measures in place.

Our national exposure research focuses on understanding these risks across East Africa, specifically in Kenya, Tanzania, and Uganda. We conduct comprehensive assessments of each country's internet landscape to identify vulnerabilities and attack surfaces and paths. Amid global challenges, including economic uncertainties and geopolitical conflicts, the iShield 360 Research Team delivers a data-driven analysis of the shifting risk landscape. We assess the prevalence and distribution of vulnerabilities in interconnected technologies that impact financial institutions, fintechs, and the wider digital payments ecosystem.

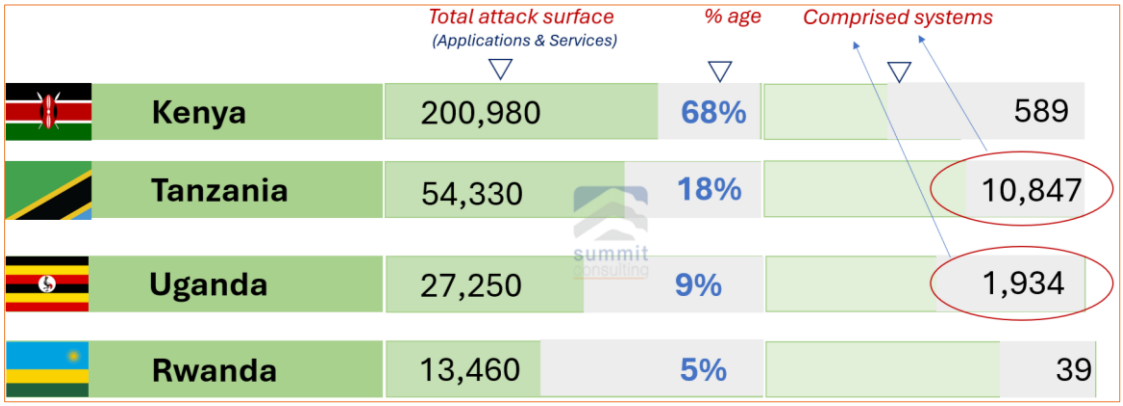
Through our findings, we offer critical insights into the cybersecurity challenges facing the region and provide recommendations to help organizations build stronger defenses against evolving threats.

1.1 Attack surface at the EA level

The East African (EA) attack surface is based on the composition of technologies that comprise the networks of all organizations and networks based within that geographical location. It encompasses all vulnerabilities, entry points, and potential exposures across the organization's network, reflecting the total area or components susceptible to cyber attacks. The exposure applies to individual organizations, industrial sectors, and at the national level.

In this section, find detailed attack surface profiling of EA-based systems and applications discovered by the iShield 360 Team cyber security research. Figure 1 highlights the discovered applications and services running on the internet in each respective country.

Figure 1: Kenya has the highest total attack surface in terms of discovered applications and services



Kenya has the highest number of exposed systems and applications, with over 200,980 discovered. As the region's digital hub for global tech giants like Microsoft, Google, IBM, and Amazon, Kenya's extensive infrastructure offers an expansive attack surface. This includes critical systems across public and private sectors, making up 68% of the region's total exposure. The sheer volume of active digital services provides ample opportunities for malicious actors. Imagine a vast network of doors and windows left partially open. That is Kenya's cybersecurity landscape.

Tanzania, with 54,330 exposed services, holds 18% of East Africa's cyber exposure. While smaller than Kenya, Tanzania's digital growth is significant. The country's systems and applications are in a phase of steady expansion, but the lack of rapid infrastructure development keeps it moderately exposed. Like a building under construction, with incomplete walls and open access points, Tanzania's digital infrastructure remains vulnerable as it grows.

Uganda, with far fewer exposed systems, reflects its early stage of digital adoption. Most innovations are still in development, hindered by limited financial resources. This lower exposure offers a temporary shield, but as Uganda's digital ecosystem matures, so will the risks. Think of Uganda as a city with emerging streets but fewer surveillance cameras. Safer for now, but increasingly vulnerable as more systems come online.

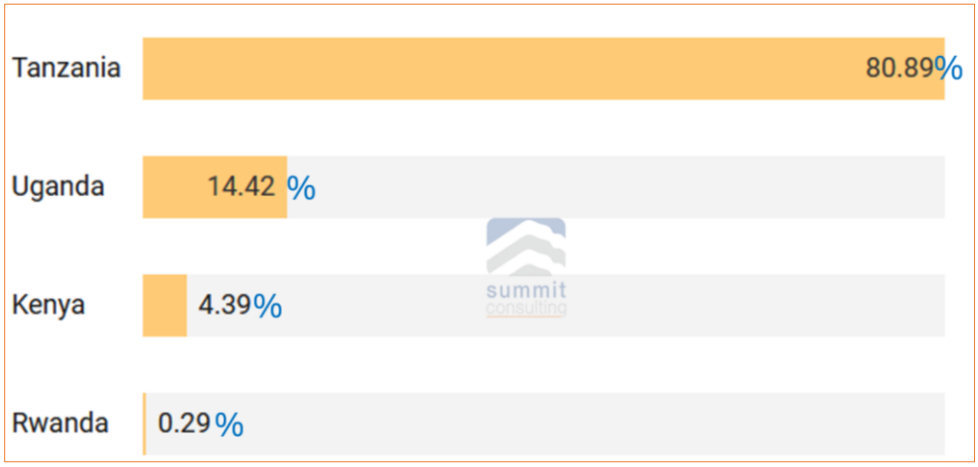
Rwanda is just starting its digital journey. With a smaller number of systems, it has the opportunity to build robust cybersecurity defenses from the ground up. Rwanda's focus on capacity building and core cybersecurity practices positions it well to secure its digital future. It's like designing a fortress before the city grows, a chance to prevent vulnerabilities before they become unmanageable. In all cases, the region's expanding digital infrastructure presents a fertile ground for cybercriminals. Our findings emphasize the importance of proactive defenses and robust cybersecurity frameworks as these countries continue to digitalize

East Africa's rapidly expanding digital landscape calls for immediate cybersecurity attention. The increasing exposure of systems in Kenya, Tanzania, Uganda, and Rwanda presents both

risks and opportunities. Now is the time to fortify defences for increased digital trust in the digital ecosystems. Conduct regular vulnerability assessments, adopt a Zero Trust Security model, and ensure that cybersecurity is embedded at every level. The iShield 360 Readiness Assessment can help evaluate your current cybersecurity posture and identify gaps before malicious actors do. Our tailored training programs for executives and leaders will equip you with the knowledge to transform your digital trust.

1.2 Tanzania and Uganda with the most comprised applications and systems in the EA

Figure 2: Tanzania with the highest percentage of applications and systems compromise. The percentages are based on the compromised systems.



Tanzania is facing the highest exposure to system compromises in East Africa. According to the iShield 360 Team's research, 10,847 out of 54,330 identified systems and applications are compromised due to weak cybersecurity defences. This is like leaving the gates wide open in a heavily trafficked area, making it easy for criminals to infiltrate.

Uganda ranks second, with 1,934 compromised systems out of 27,250. Though smaller in scale, Uganda's compromised systems reveal vulnerabilities that make it a prime target.

Surprisingly, Kenya, with the largest digital footprint at 200,980 systems, has fewer compromised systems at 14%. This demonstrates that while Kenya's attack surface is vast, its cybersecurity practices, though far from perfect, are more robust than expected. It's like a large mansion with a tall and strong perimeter fence and fewer gates and doors, making it harder for attackers to find an entry point.

Rwanda performs the best in cybersecurity resilience. With only 39 compromised systems out of 13,460, Rwanda has managed to secure its digital infrastructure effectively. It's like building a fortress with fewer vulnerabilities from the start, giving attackers little room to manoeuvre.

The lesson is clear: size doesn't necessarily correlate with risk. It's the quality of defences that determines the level of exposure. Whether you are operating 200,000 systems or 2,000, strong cybersecurity measures make all the difference. Ethical hacking practices like

penetration testing and regular vulnerability assessments are critical for identifying weak spots before attackers do. Act now. Don’t leave your organization’s digital doors open to threats. Conduct a full cybersecurity audit, implement stronger controls, and invest in resilience.

summit