



Think Outside
the Firewall™



Standard Bank

Standard Bank Improves Digital Asset Management and Threat Protection with RiskIQ

Challenges

- Rapid pace of change for digital presence across multiple channels
- Lack of visibility needed to manage the security of digital assets
- Malicious copies of mobile applications

Solution Benefits

- Automatic discovery and analysis of new and changed online assets
- Central visibility of digital assets to detect possible indicators of compromise
- Continuous monitoring of suspicious domains
- Discovery and scanning of mobile applications across 180+ app stores

“The intelligence provided by RiskIQ has enabled visibility and collaboration between our central and decentralized teams to continually improve our security posture and protect the bank and our customers from cyber threats.”

– Robin Barnwell
Head: PBB IT Security
Standard Bank

About Standard Bank

Standard Bank Group is the largest African banking group by assets, offering a full range of banking and related financial services. With a heritage of over 150 years, they have a presence in 20 countries across the African continent, as well as in other selected emerging markets. Standard Bank is committed to creating a fully digital bank across all of these geographies.

Challenges

Standard Bank's digital journey has increased their online presence across web, mobile, and social channels. As with many financial organizations, protection against brand infringement, cybercrime, and web-based attacks is a top priority.

The pace of change and digital development programs running across multiple countries created a challenge for the central security team, as they lacked the visibility needed to bring all digital assets under the scope of their security program.

Another problem was related to legitimate mobile applications published in the primary app stores being copied and published through secondary and affiliate app stores. These copies could be modified to be malicious, leading to brand and customer impact.

The security team was looking for a solution that could automate the discovery and threat analysis of the full digital presence, to replace the manual processes.

Key considerations included:

- Providing automated digital asset discovery, including cloud and third-party hosted sites, to ensure that the view of their digital channels is up to date.
- Allowing granular risk views for asset owners.
- Supporting the marketing team for the management of social media assets and domain infringements.
- Allowing for easy integration into existing monitoring and reporting tools.
- Supporting ongoing initiatives such as data privacy.

The RiskIQ Solution

Standard Bank selected RiskIQ as their digital threat management partner, using both RiskIQ Digital Footprint™ and RiskIQ External Threats™ solutions.

RiskIQ Digital Footprint continuously scours the web to discover new and updated digital assets, based on attributes like IP range and name and brand recognition. It also provides in-depth information about those assets and highlights potential risks. The Standard Bank security team uses this information to get central visibility of digital assets and ensure compliance with corporate standards, wherever the site is hosted. Digital Footprint also gives a view of new redirections appearing on webpage links that might be an indication of compromise.

The security team has also used RiskIQ's intelligence to clean up domain and certificate registrations including standardizing contact details across registrations, ensuring that key communications such as renewal notices are not missed. They have also been able to identify and update older untrusted certificates across their web estate.

To uncover brand-related threats, Standard Bank is using Mobile Threats and Domain Infringement, both part of RiskIQ's External Threats solution. Using the intelligence provided by Mobile Threats, the security team can track where apps are published and request the removal of apps that end up in unauthorized stores. They are also able to identify and track mobile apps not owned by them that leverage their brands and issue takedown requests where the risk is unacceptable.

Standard Bank is using the Domain Infringement module to identify newly registered domains that infringe on their brand and which could potentially be used for squatting or phishing campaigns. RiskIQ continually monitors suspicious domains, and the security team is alerted when changes occur—for example, a parked site going live.

In conjunction with the marketing team, the security team have recently started monitoring their social media accounts including corporate accounts, brand accounts, and the social profiles of key executives. Fake social accounts are commonly used in phishing and credential-harvesting campaigns and can affect user trust and brand perception.

The Results

Using RiskIQ solutions, the Standard Bank security team has gained visibility of its digital presence across web, mobile, and social channels and can work with the business to proactively address areas of weakness.

"The intelligence provided by RiskIQ has enabled visibility and collaboration between our central and decentralized teams to continually improve our security posture and protect the bank and our customers from cyber threats," said Robin Barnwell, Head: PBB IT Security. "RiskIQ has now become the CMDB for our Digital Footprint assets."

Next Steps

Working with the RiskIQ customer success team, Standard Bank is looking at integrating RiskIQ solutions with other security solutions to further improve automation and reduce manual tasks. They are also looking at additional areas where RiskIQ could add value, including compliance with data privacy regulations (GDPR/POPI), risk scoring, and benchmarking.

Conclusion

RiskIQ's Digital Footprint and External Threat solutions combine advanced internet reconnaissance and analytics and an integrated toolset to provide automated attack surface visibility and targeted brand-threat protection.



RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

✉ sales@riskiq.net 🌐 RiskIQ.com

☎ 1 888.415.4447 🐦 @RiskIQ

Copyright © 2018 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 03_18

The only warranties for RiskIQ products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. RiskIQ shall not be liable for technical or editorial errors or omissions contained herein.