telenor microfinance bank

STRONGESTLAYER

Telenor Microfinance Strengthens Email Stack Against AI Cyber Threats with Next-Gen In-Workflow Analysis and Training

01 The Customer

Telenor Microfinance Bank is a high-tech, innovative financial institution that focuses on promoting financial inclusion through digital banking solutions. It stands out for integrating groundbreaking technologies like blockchain for secure cross-border remittances and being a leader in digital lending via its Easypaisa platform. The bank's commitment to advancing financial services and its strategic partnerships enable it to drive digital financial transformation and maintain a leadership role in the banking sector

02 The Challenge

SOC Overload	Ineffective Training	Threat Visibility Gap
The SOC was overloaded by suspicious emails landing in their users' inboxes. These attacks consistently bypassed their Secure Email Gateway, requiring constant, in-depth manual triage. Both their inboxes and users remained vulnerable to AI generated phishing and browser-based threats.	Users were being assessed using out of date phishing simulations based on pre-loaded templates. Telenor needed to understand how their users would respond to the 'next threat' unknown to the Telenor SOC or other security vendors. This is a critical part of building true cyber resilience.	The team lacked visibility into how users were being targeted by AI-Generated, pre-weaponized threats, making it difficult to build effective cyber resilience programs and provide detailed reports on the evolving threat landscape.

03 The Solution

Real-Time AI Threat Detection: AI-powered threat analysis provided instant insights within end user workflows, delivering actionable intelligence to mitigate risks before they escalated.

Streamlined SOC Email Triage: StrongestLayer's integration streamlined email management for the SOC, helping identify high-risk messages and protect users from phishing and web-based threats.

Next Generation Response Assessment: Automated phishing simulations trained employees to detect evolving threats, improving Telenor Microfinance's human layer security.

StrongestLayer was deployed as a comprehensive solution to address Telenor Microfinance’s email security and human risk challenges. With **CyberGuard** integrated into employees workflows, the platform simplified email triage for the SOC, identifying high-risk messages and safeguarding users from phishing and browser-based threats.

StrongestLayer’s AI-powered detection provided real-time analysis of threats within a user’s workflow and **delivered actionable threat intelligence to mitigate risks before they could escalate.**

The platform also introduced **automated, threat intelligence-driven phishing simulations** to train employees and test their ability to detect future phishing attempts, further enhancing the bank's human layer security. By integrating **CyberGuard** into the email workflow, Telenor Microfinance effectively reduced the risks from both email and web threats.

04 The Results

Strengthened Defense Against Advanced Email Threats

Significant boost in ability to combat suspicious emails that bypass the Secure Email Gateway, streamlining SOC email triage in the process.

Improved SOC Visibility and Continuous Reporting of Cyber Resilience

Improved visibility into targeted attacks, enabling the SOC team to identify at-risk users and report cyber resilience continuously to leadership.

Enhanced Employee Cyber Resilience Through Realistic Phishing Simulations

Increased employee resilience to cyber threats through realistic, forward-looking phishing simulations and interaction with the in-workflow assistant

05 Conclusion

By adopting StrongestLayer, Telenor Microfinance effectively closed the gaps in their email security systems, significantly reducing the risks posed by email and browser-based threats. With the **CyberGuard Plugin** safeguarding their users, the bank gained critical visibility into AI generated, targeted threats while empowering employees to act as a critical line of defense. StrongestLayer not only improved their immediate email security requirements but also fostered a culture of security awareness through continuous user training and threat simulations while heavily reducing the amount of time the SOC spends triaging suspicious email.

06 Testimonial

"We are thoroughly impressed with StrongestLayer and highly recommend them to any organization looking to strengthen their defenses against phishing attacks. Their focus on human layer security demonstrates a deep understanding of the critical role individuals play in an organization's overall security. StrongestLayer's detection and threat intelligence capabilities are outstanding. They consistently identify and mitigate malicious, phishing, and risky emails with impressive accuracy. Their advanced AI-driven phishing campaigns are both highly effective and realistic! We are loving StrongestLayer!"

— Khizar Ahtisham, Information Security Expert, Telenor Microfinance Bank