Executive Summary

2025 Security Annual Report

In 2025, we drove continued optimization as AI fundamentally changed the way we operate. We embraced AI tools to streamline and automate security processes, while enabling the secure use of AI across the business. We also mitigated adversarial AI, deploying custom controls to block quickly evolving threats. We further integrated our Security and Technology teams for greater speed and efficiency internally, and we continued our commitment to transparency and collaboration between businesses and governments externally.

Actions

Modernized our Approach to Security Culture

We enhanced our security culture by launching gamified AI training, increasing phishing simulations, adding six new role-based behaviors to security scorecards, and adopting a new phishing reporting tool to better identify malicious indicators.

Reinforced Security as a Market Differentiator

We supported the secure launch of a record number of NPIs in 2025, while obtaining 52 certifications including critical U.S. government authorizations. A new AI knowledge base now automatically generates responses to security questionnaires, helping our teams meet customer needs with speed.

Unified Security and Engineering

We combined our Security Architecture and Technology Architecture functions, and provided them with an automated development platform to securely ship 50% more changes. We covered 164% more critical infrastructure components while maintaining an average issue closure time of < 24 hours.

Co-Innovated with Vendors and Partners

From endpoint protection to cloud services to identity and access management, we partnered with our security vendors to shape product and service enhancements that drive industry standards forward.

Advanced Security in an AI Age

We deployed AI as a strategic force multiplier, upgrading our ability to remediate threats and accelerate critical security decisions. We also built guardrails like automated content safety filters and secure coding frameworks that allow our teams to adopt powerful new tools without exposing the enterprise to unmanaged risk. Across the enterprise, we recalibrated our defenses to detect and protect against new and evolving AI-enabled threats.

19.8M+ Cyber threats defended against on average each day

240,000+ Simulations to test our global workforce in security

2,280+ Deep-dive risk analyses on critical risk third-party vendors

330+ Automated cloud security checks monitored in real time

180+ New Product Innovations (NPIs) securely brough to market

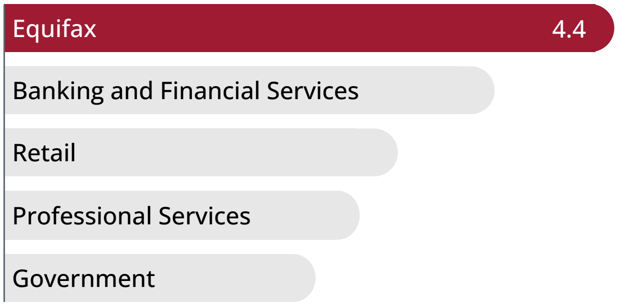
18 Tabletop exercises simulating crisis scenarios

1 min Mean time to detect cyber threats

Security Maturity Score

An organization's security maturity characterizes how well it can adapt to cyber threats and manage risk over time.

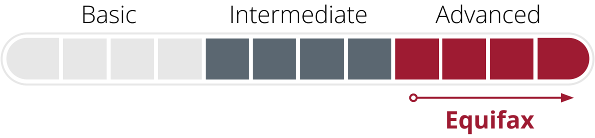
The maturity of our cybersecurity program, with a 2025 National Institute of Standards and Technology (NIST) Cybersecurity Framework score of 4.4, improved in 2025, outperforming all major industry benchmarks for the sixth consecutive year.



Security Posture Rating

An organization's security posture reflects its readiness and ability to identify, respond to, and recover from security threats and risks.

At year-end 2025, our security posture rating exceeded Technology and Financial Services industry averages for a fifth consecutive year.



These are the rating categories assigned by the reporting service that monitors our posture. Equifax maintains a rating that places us in the highest category.

View the full report at **equifax.com/newsroom**