Security

Annual Report

EQUIFAX®

Table of contents

We have truly built one of the world's most advanced and effective cybersecurity programs. At the same time, we recognize that our work in security is never done.

– Mark Begor

A message from Equifax CEO

Mark Begor

Mark W. Begor

Chief Executive Officer
Equifax

2024 marked an energizing chapter of transformation and growth for the New Equifax. We made significant progress towards the completion of our data and technology transformation. As we look ahead, we are building on the strong foundation of the Equifax Cloud™ and our EFX.AI capabilities to drive innovation, new products, and future growth. Importantly, strong cybersecurity is core to each of our business actions.

When I joined Equifax in 2018, I made a personal commitment to establish the company as an industry leader in security and to build a culture where security is part of our global team's DNA — where everyone in Equifax owns security. Since that time, we have transformed our organization at every level to deliver on that promise. In 2024, the maturity of our cybersecurity program outperformed all major industry benchmarks for a fifth consecutive year. And our security posture score continues to exceed Technology and Financial Services industry averages.

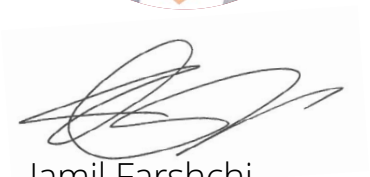
With the release of our fifth Security Annual Report, we celebrate our security progress to date. We have truly built one of the world's most advanced and effective cybersecurity programs. At the same time, we recognize that our work in security is never done.

2024 saw a host of new threats to global cybersecurity infrastructure. Last year, we responded to more than 15 million cyber threats — that's nearly 175 hostile attempts every second and a 25% increase from 2023. Remaining ahead of those threats requires continuous evolution and innovation. It requires us to constantly think differently, which is why I am proud of initiatives like our industry-leading passwordless transformation and our roll-out of passwordless technology across Equifax, including the use of biometrics, to help eliminate the number one threat facing security teams: stolen credentials.

As we look ahead to what's next for Equifax, security remains a critical strategic business priority. We will continue to grow and evolve our security posture and programs to meet and anticipate evolving cybersecurity threats. And we will continue to communicate transparently on our security initiatives, sharing our lessons learned for the benefit of the industry at large.

A message from Equifax CTO & CISO

Jamil Farshchi



Jamil Farshchi

Chief Technology Officer and Chief Information Security Officer
Equifax

We often hear, "You can't have great security and rapid innovation." In 2024, we decided to debunk that myth. We witnessed a continued increase in AI-driven threats and geopolitical tensions, making the cybersecurity landscape more concerning than ever — but we didn't stand still. We modernized our defenses, accelerated cloud adoption, and pushed the boundaries by tackling the most significant cause of breaches: compromised credentials.

That's right — this year, we moved our entire workforce of nearly 22,000 employees and contractors to passwordless authentication for about 300 internal applications. It wasn't just a bold idea to protect us against stolen passwords; it also slashed help desk costs, improved workforce productivity, and future-proofed our defenses against AI impersonation tactics like voice cloning. In one shot, we improved user experience and security outcomes.

At Equifax, we don't believe in the false "security vs. speed" tradeoff. Our results speak for themselves: We launched more than 100 new product innovations (NPIs) in 2024 while sustaining a security maturity score that once again beat major industry benchmarks. This year's Security Annual Report is our fifth in a row — a testament to our commitment to transparency, collaboration, and continuous improvement.

Throughout this journey, we've open-sourced our controls framework, exposed our real-time cloud security posture to customers with CloudControl, strengthened public and private partnerships, and shared our insights with the entire community.

Am I satisfied? Absolutely not. We know adversaries are constantly upping their game, leveraging zero-day exploits, supply chain weaknesses, and, more recently, AI — to find new footholds. Our response is to double down on security. And security is no longer a conversation about "slowing the business" — it's now front and center in fueling our momentum and growth.

In 2024, customers cited our security reputation as a key reason they chose Equifax. Our product velocity and stability reached a record high this past year. And we have a lot more to accomplish, but one thing is clear: **Security and innovation aren't mutually exclusive.**

As we look forward, we'll keep pushing boundaries, dismissing outdated thinking, and doing what it takes to be the best at defending consumers' data *and* enabling bold innovation at Equifax. Thank you for being on this journey with us.

Our impact

Equifax Security in 2024

15 million+
Cyber threats defended against each day — nearly 175 hostile attempts every second, a 25% increase from last year.

210,000+
Simulations launched to test our global workforce on diverse security scenarios.

~22,000
Employees and contractors trained with personalized security modules, achieving our lowest click rate ever (2.9%) in targeted phishing simulations.

3,550+
Customer questionnaires and audits completed to reinforce confidence in our security posture.

4,200+
External users accessed our security and privacy controls framework across more than 80 countries.

2,250+
Deep-dive risk analyses on critical and high-risk third-party vendors, identifying potential security flaws before they can be exploited.

700+
Organizations supported via Equifax Breach Services, offering identity protection to over 22 million breach victims globally.

450+
Dedicated cybersecurity professionals protecting consumer data around the clock.

370+
Automated cloud security checks monitored in real time, fueling faster threat response and near-instant posture awareness.

100+
New Product Innovations (NPIs) securely brought to market — proving speed and security aren't at odds.

51
Certifications and authorizations obtained from outside auditors, validating our depth and rigor.

38
Physical security assessments completed to protect our people, data, and assets.

30+
Forums participated in globally to share intelligence and strengthen collaborative defenses.

15
Tabletop exercises simulating crisis scenarios at the executive and regional levels.

5
Consecutive years hitting a Security Maturity score that outperforms all major industry benchmarks.

2
Acquisition integrations completed under a new, streamlined security playbook.

<1
Minute mean time to detect cyber threats — because we don't let adversaries linger.

State of play

Cybersecurity in 2024

The themes below are representative of the prevalent themes of the past year, and how Equifax has responded.

Supply Chain Attack Velocity

In 2024, supply chain attacks surged in frequency and sophistication, fueled by our reliance on interconnected systems. A single compromised vendor can ripple through entire ecosystems, with global projections estimating up to $138 billion in damages annually by 2031.[1]

Our approach? Zero trust, M&A security framework unification, and real-time visibility expansion into third-party risk. We're also trying to help where Equifax *is* the third party. Through our CloudControl dashboard, customers gain continuous insight into Equifax Cloud™ product security, empowering them with the information they need to make informed risk decisions.

Zero Day Vulnerabilities and Infrastructure Exploits

With AI-assisted vulnerability discovery taking off, zero-day exploits targeted both core software stacks and network devices. Criminals leveraged newly found flaws — often sold on underground marketplaces — to plant ransomware or establish stealth footholds. Many firms struggled to patch quickly enough, reinforcing the importance of fundamentals like consistent scanning and comprehensive patching protocols.

We responded by pushing continuous monitoring coverage, aggressive perimeter patching, and slashing our response times down to minutes, preventing attackers from capitalizing on these openings.

Credential Theft + AI-Driven Social Engineering

Throughout 2024, attackers ramped up AI-based impersonation — deepfake voices, realistic phishing, and targeted social engineering — to exploit the human factor. Credential theft already accounts for a majority of breaches, but voice cloning elevated help desk fraud into a major threat.

Equifax tackled this head-on by rolling out passwordless authentication for nearly 22,000 employees and contractors — addressing one of today's top breach vectors. We also implemented passwordless for help desk calls — mitigating a top emerging cyber threat: AI-based voice cloning. Coupled with zero-trust principles and over 210,000 workforce social engineering simulations, we've leaned in to defend against the top risks of today and tomorrow.

Ransomware Evolution

Ransomware attacks evolved beyond simple data encryption in 2024. Operators refined multi-stage attacks, halting operations, stealing data, using double or triple extortion techniques... even trying to fake a breach to compel payment. A single, large-scale hit can result in countless losses and negatively impact downtime and recovery.

At Equifax, we counter adversaries with a layered defense — advanced endpoint detection, automated patch prioritization, zero-trust architecture, and robust backup processes. None of it is perfect, but we're working tirelessly to continually improve in all areas.

[1] Cybersecurity Ventures (2023, October 03). Software Supply Chain Attacks To Cost The World $60 Billion By 2025. EIN Presswire. https://world.einnews.com/pr_news/659375862/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025

Our actions

Equifax Security initiatives and results in 2024

Strengthened Our Culture of Security Ownership

We made it easier than ever for our employees and contractors to keep putting security first by increasing education and reducing friction.

Our employees and contractors excel at recognizing and avoiding suspicious links. We conducted over 210,000 global phishing simulations, achieving our lowest click rate ever for simulated phishing emails.

We made logins at Equifax quicker *and* more secure than ever by deploying passwordless authentication to all of our nearly 22,000 employees and contractors globally, mitigating one of the top security threat vectors.

Security is everyone's job at Equifax. We all own security and each of our employees and contractors are trained, empowered, and incentivized to treat it as a personal priority — one that fosters trust and speed.

Enhanced Technology and Security's Partnership

In 2024, we went all in on strengthening our partnership between our Technology and Security functions.

We merged Tech Infrastructure with Security Operations and Business Continuity and Disaster Recovery (BC/DR) with Security Crisis Management — **unifying our ability to execute and respond.**

Disproving the myth that security stifles innovation, we launched over 100 NPIs in 2024 with integrated security from the ground up.

These and other optimizations ensured a more **seamless and efficient execution,** unlocking synergies that enable security to accelerate (instead of slowing down) product launches.

Advanced Our Operational Excellence

We continued to refine our tools, data, and personnel to maximize their impact.

Employing AI-driven enhancements, we accelerated penetration tests, application reviews, and log analysis for improved threat detection, all while maintaining human oversight.

This focus on continuous improvement yielded significant results. Our cybersecurity team **reduced threat response times by 60%-99% year over year,** as measured by the time to detect, respond to, and resolve incidents.

Similarly, our Physical Security Operations Center streamlined processes and leveraged automation to achieve a **33% improvement in response time to high-priority local alarms,** now averaging under two minutes.

Continued

Equifax Security initiatives and results in 2024

Minimized Supply Chain Risk

We enhanced our supply chain security at every level.

We incorporated supply chain metrics into relevant Equifax employees' monthly Security Snapshots. This targeted behavior measurement further emphasized the importance of our people's part in protecting Equifax through proper evaluation of vendor connections and relationships.

And we **retooled our vendor security validations**, measuring new data points that reveal how third parties handle emerging risks.

To **enhance our customers' access and visibility into Equifax products,** we launched the mobile-friendly version of our CloudControl dashboard — a first-of-its-kind solution that provides continuous insights into Equifax Cloud™ product security posture.

Scaled External Collaboration

In 2024, we kept pushing to make transparency and collaboration between businesses and governments a global norm.

Equifax CTO & CISO Jamil Farshchi co-hosted the FBI's new cybersecurity podcast miniseries with the head of the FBI's Cyber division, demystifying law enforcement support.

Our team partnered with the governments of Costa Rica and Chile to help bolster security, bridging public-private gaps internationally.

And we continued to champion open communication to stay ahead of the next generation of global threats.

Boosted the Bottom Line

Good security is good for the bottom line — and in 2024, we helped drive business objectives at every level.

Security is no longer just focused on basic compliance, but also helping drive new revenue, as **customers cite our security leadership as a key reason they chose Equifax.**

And we achieved Data Privacy Framework (DPF) certification, affirming our commitment to securely facilitating international data transfers from the EU to the US.

A blueprint for eliminating credentials

Second half 2023

Tech Support Calls

Industry Standard	Our Approach
The industry has seen social engineers zero in on help desk access Cyber criminals target companies by impersonating employees to gain privileged access, often tricking technical support staff via phone calls, exploiting easily obtainable "security questions" (e.g., mother's maiden name). **No unified out-of-the-box solution** There was no existing single solution available that reliably and sustainably addressed this vulnerability.	**New way to authenticate for tech support calls** We identified an upstart vendor and worked with them to fine-tune the best solution to address this vulnerability — implementing an application-based Interactive Voice Response (IVR) solution that enabled employees to automatically authenticate when calling Equifax technical support. **Easing users into passwordless** We first deployed this tool for help desk access, to both minimize workforce disruption and shut down a significant risk vector. It would later be used for passwordless web app and VPN access.

First half 2024

Laptops and Desktops

Industry Standard	Our Approach
Password-based logins Users access laptops and desktops by authenticating with traditional “username and password” protocols. **No third party app involved** Device logins depend entirely on authentication mechanisms built into operating systems, without the involvement of third-party solutions. **Biometrics not enabled** Common infrastructure constraints prevent the widespread use of biometric authentication functionality.	**Device login configuration changes** We guided users through the actions necessary to enable passwordless workstation logins through biometric authentication. **Phased rollout** We implemented this method to a few hundred users at a time over several months, allowing for iterative trouble-shooting and tailored communications. **Foundation for subsequent components** These configuration changes were essential building blocks for the upcoming passwordless implementations (web apps and VPN).

Continued

A blueprint for eliminating credentials

Second half 2024

Web Apps and VPN

Industry Standard

Centralized web app access (SSO)
Users access web apps (such as email, collaboration tools, and other business-critical systems) via a central Single Sign-On (SSO) system.

Securing web apps with MFA
This SSO is secured by a password and Multi-factor Authentication (MFA).

Securing network with MFA
Access to the Virtual Private Network (VPN) is protected by MFA, requiring users to enter a password when connecting to Wi-Fi remotely, followed by a mobile device-based verification.

Critical first step
Password-protected VPN logins are the essential first step before accessing any company resources, making password issues particularly disruptive.

Anticipated transition challenge
Due to its critical nature and impact on the remote workforce, migrating systems for credentialed VPN access is likely to be disruptive for end users.

Our Approach

Passwordless integration
We integrated our existing Single Sign-On (SSO) system with a passwordless authentication service, enabling users to authenticate into the VPN and certain applications using their mobile devices. Workstations also enabled biometric authentications.

Started with opt-in/nudges
We began with an opt-in approach, allowing users to voluntarily switch to passwordless. From there we progressively moved from nudges and reminders to a full default to the passwordless method.

Comprehensive communication
We communicated the transition early and often across numerous channels (email, intranet posts, digital signage, etc.) and included both technical instructions and value communication. We made sure every employee understood the benefits of a passwordless workflow!

Collaboration

Our key to a successful passwordless transformation

The benefits of a passwordless environment are indisputable. But the challenges of transitioning away from the status quo can be daunting. Changing established behavior patterns is hard. Collaboration was the force multiplier that made this transformation possible.

Co-innovated with our vendor

We saw the potential of passwordless technology to minimize risk and increase convenience. With these benefits in mind, we made a calculated decision to support the technology's development during its formative stages, forging an interactive feedback loop with our vendor. This transformative partnership enabled breakthroughs (such as a new IVR verification process for tech support calls) that are now helping to drive industry-wide adoption. Other financial services organizations are already beginning to embrace this path, which will lead to systemic security improvements across the global supply chain.

Tech and Security partnered closely

This initiative epitomized the value of our Technology and Security Teams' strong collaboration. They partnered intimately from planning to execution, ensuring both user experience and security were addressed at every stage of this transformation.

Entire workforce played a role

Each of our employees and contractors treats security as a personal responsibility, and their commitment was crucial to the success of this transformation. They weren't passive recipients of change — they were active collaborators in its implementation. Everyone adapted their daily workflows to integrate the new system. This included adjusting to new authentication methods, embracing biometric logins, and adopting the mobile authentication application. Their willingness to embrace change was instrumental in creating a seamless and efficient transition, helping enhance our security.

Not "one size fits all"

Equifax is a global company and our regional Security and Technology Teams played a pivotal role in not only helping deploy our new passwordless technology but also in helping empower our entire workforce. They provided personalized support, addressed unique local challenges, and delivered tailored training programs. This localized approach ensured that every employee, regardless of location, felt supported and equipped to embrace this transition.

We're excited to keep the collaboration going in 2025 and beyond, hosting knowledge-sharing sessions with customers and partners who aim to replicate our enterprise passwordless transformation.

Independent benchmarking

Security Maturity

We partner with a leading global research and advisory firm to conduct an objective in-depth analysis of the maturity of our entire security program.

Security Maturity Score

What is Security Maturity?

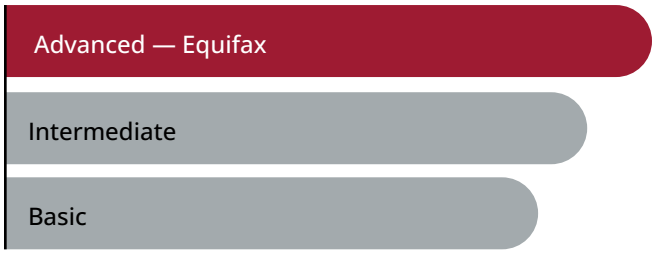
An organization's security maturity represents how well it can adapt to cyber threats and manage risk over time.

We maintained leadership with the maturity of our cybersecurity program in 2024, outperforming all major industry benchmarks for a fifth consecutive year.

Security Posture

A leading cybersecurity reporting service continuously monitors the posture of our security program and assesses the risk of our supply chain ecosystem.

Security Posture Rating



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.

What is Security Posture?

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

Our security posture score exceeded Technology and Financial Services industry averages for a fourth consecutive year.

Summary of results

Equifax Security in 2024

Security Posture and Maturity

- Achieved a best-in-class maturity rating for operating a security program aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), outperforming all major industry benchmarks for the last five years.
- Achieved a Security Posture rating that exceeded technology industry benchmarks for a fourth consecutive year.

Cybersecurity

- Monitored 374 cloud security checks in real time, improving our posture visibility.
- Enforced Multi-factor Authentication (MFA) for 100% of remote access, reducing unauthorized entry risks.
- Transitioned to passwordless logins for our nearly 22,000 employees and contractors globally, neutralizing credential-based threats.
- Improved threat response times by 60%-99% year over year, thanks to AI-based detection, process optimization and integrated threat intelligence.

Compliance

- Successfully obtained 51 certifications with a 6% year-over-year cost reduction, demonstrating $500,000 in savings in 2024 alone.

M&A

- Integrated two previous acquisitions to near completion using our repeatable framework, with 94% of controls meeting Equifax standards.

Risk Management

- Performed deep-dive risk analyses on 100% of our company's critical and high-risk third parties (2,253).
- Completed risk assessments on 100% of business applications (6,308).
- Launched a mobile-friendly version of CloudControl for continuous cybersecurity posture visibility.

Privacy

- Implemented a new tool for email data loss prevention (DLP), enhancing user insights and data protection.
- Published a global Job Applicant Privacy Statement to clarify personal data handling.
- Obtained Data Privacy Framework (DPF) certification, enabling secure EU/UK to US. data transfers.

Continued

Equifax Security in 2024

Crisis Management

- Conducted 15 tabletop exercises with real-time crisis simulations with company stakeholders, including:
  - CEO and Executive Team
  - Regional and Business Unit Crisis Teams
- Introduced new tabletops focusing on workplace safety, disaster recovery, and Form 8-K scenarios. A Form 8-K is a report that must be filed with the U.S. Securities and Exchange Commission (SEC) to announce significant events.
- Implemented customized regional and business unit specific crisis plans.
- Expanded our crisis preparedness footprint by establishing local crisis teams for our Dominican Republic and Brazil operations.

Security Training

- Conducted over 210,000 simulations, achieving our lowest-ever click rate for simulated phishing attempts: 2.9%.
- Incorporated supply chain metrics into relevant employees' monthly Security Snapshots, further emphasizing the importance of their part in protecting Equifax through proper evaluation of vendor connections and relationships.

Breach Services

- Supported more than 700 organizations responding to cyber incidents; on behalf of our clients, offered ID protection to 22 million breach victims in over 25 countries.

Customer Engagement

- Completed 3,551 questionnaires and audits at the request of Equifax customers to ensure compliance.
- Securely brought over 100 NPIs to market for the fifth consecutive year.

Fraud

- Enhanced our fraud detection, triggering 41% more suspicious activity escalations than in 2023, demonstrating heightened visibility and stronger mitigation strategies.

Physical Security and Investigations

- Completed 12 physical penetration tests, identifying continual improvement areas.
- Conducted 38 physical security assessments to secure employees, data, and assets.

Our path forward

In 2024, we leveraged Security as an engine for speed, trust, and market differentiation — cutting out credentials, fusing AI into threat detection and day-to-day operations, and turning adversity into advantage. We're not just playing defense; we're moving faster, launching new products, and setting the bar higher than ever. And we're not done. As we move into 2025 and beyond, we're focused on continued innovation. We will continue to forge new paths in security and technology to help us safeguard our customers' data against malicious actors and share for the benefit of the industry at large.

1550 Peachtree Street NW, Atlanta, GA 30309 • 404.885.8000 • equifax.com