EQUIFAX®

Security
Annual Report
2025

Table of contents

We believe that more communication, more collaboration, and more transparency, equals stronger security.

A message from Equifax CEO

Mark W. Begor

Mark W. Begor

Chief Executive Officer
Equifax

2025 was an energizing year of growth and innovation. With our $3 billion global security and technology transformation — and the creation of the Equifax Cloud™ — principally complete, EFX.AI is powering the future of the New Equifax. We are ramping the deployment of patented EFX.AI technology in our products, leveraging the unique and proprietary data that sets Equifax apart in the industry. This has driven a record number of New Product Innovations (NPIs) that deliver the decision intelligence our global customers need to create new opportunities faster than ever before. And, we are gaining efficiencies by leveraging AI internally to spend less time on routine items and more time on the complex, creative, and collaborative challenges that drive our company forward.

Our unwavering commitment to security sets a strong foundation for this innovation.

When I joined Equifax in 2018, I made a personal commitment to establish Equifax as an industry leader in data security, and to build a culture where everyone in Equifax owns security. We have transformed every aspect of our organization to deliver on that promise, making security part of our global team's DNA. With the release of our sixth Security Annual Report, our relentless focus on security leadership is clear: our security maturity level has outperformed all major industry benchmarks for six consecutive years, and our security posture score has exceeded Technology and Financial Services industry averages for a fifth consecutive year.

At the same time, we recognize that our work in security is never done.

2025 saw a host of new threats to global cybersecurity infrastructure, defined by a convergence of volume, speed, and AI-powered sophistication. We saw autonomous agents and industrialized AI amplify traditional attacks, expanding the scope of what we must defend. Equifax was ready. Guided by our focus on relentless optimization, and maximizing our cloud-native infrastructure, we defended against more than 19.8 million cybersecurity threats each day while conducting more than 240,000 simulations to test our global workforce and prepare for what's ahead.

While many companies are expected to be disrupted or disintermediated by AI, Equifax is leveraging AI to disrupt the industry and accelerate our security leadership. We are proud that AI has fundamentally changed how we operate, with almost 90% of our global team leveraging AI tools in 2025. As we empower our business to innovate with AI, we have built rigorous guardrails — from automated content safety filters to secure coding frameworks — ensuring our models are explainable, safe, and that our proprietary data remains protected.

We will continue to leverage AI to enhance our defenses, secure the business's use of AI for innovation, and defend against AI threats. Importantly, we will not only maintain our focus on security, but also continue to help our customers, partners, and consumers strengthen their own cybersecurity postures for the benefit of the industry at large.

A message from Equifax CISO

Jeremy Koppen

Jeremy Koppen

Chief Information
Security Officer
Equifax

I came to this role with a distinct perspective on the Equifax security journey. Before joining the company as CISO in May 2025, I was a Managing Director at Mandiant, where I had the privilege of working alongside this team during the early, pivotal stages of their transformation. And for years afterward, I admired their continued progress from the outside.

I knew Equifax had been recognized as an industry leader in security. But when I walked in the door, I didn't find a team taking a victory lap. I found a team with a drive and focus that immediately stood out.

That intensity is critical because the 2025 threat landscape was defined by a convergence of volume, speed, and sophistication. We saw autonomous agents and industrialized AI amplify traditional attacks, radically expanding the scope of what we must defend. In this environment, simply doing *more* isn't a strategy. We must proactively evolve to stay ahead.

So, this year, we focused on **relentless optimization.**

AI has fundamentally changed the way we operate. Leveraging our cloud-native infrastructure, we used AI to streamline our Security Operations Center and accelerate routine tasks so our experts could focus on the threats that matter most. We also mitigated adversarial AI, deploying custom controls to block invisible prompt injections and deepfakes. And we secured the business's use of AI, architecting our systems to remove friction while building the guardrails that allowed our workforce to quickly *and* responsibly leverage AI capabilities in every corner of Equifax. This discipline helped ensure that security **remains a true business accelerator.**

The proof is in our output. In 2025, Equifax securely launched more than 180 New Product Innovations (NPIs) — our sixth consecutive year over 100. This demonstrates that rigorous security is not a competing interest, but a vital enabler of rapid innovation and growth.

Perhaps most importantly, security at Equifax is a shared discipline. We see this in action as our Technology teams build secure-by-design architecture, and as our Finance and Legal partners ask the hard questions about third-party risk. We also see it in our employees across the globe who act as human sensors, flagging novel phishing attempts and reinforcing our automated defenses with human intuition.

Are we satisfied? Absolutely not. We increased our security maturity again in 2025, but the threats we face continue to evolve. We'll continue to embrace new technologies, optimize our defenses, and prioritize our efforts based on impact, not ease.

I'm proud to lead a team with relentless ambition to outpace the status quo. Our pursuit of security leadership has no ceiling.

Our impact

Equifax Security in 2025

19.8 million+
Cyber threats blocked each day — nearly 230 hostile attempts every second, a 30% increase from last year.

240,000+
Simulations launched to test our global workforce on diverse security scenarios.

~22,000+
Employees and contractors trained with personalized security modules, increasing difficulty of simulations to mirror the evolving threat environment.

4,000+
External users accessed our security and privacy controls framework across more than 70 countries.

3,700+
Customer questionnaires and evidence requests completed to reinforce confidence in our security posture.

2,280+
Deep-dive risk analyses on critical and high-risk third-party vendors, identifying potential security flaws before they can be exploited.

400+
Dedicated cybersecurity professionals protecting consumer data around the clock.

330+
Automated cloud security checks monitored in real time, fueling faster threat response and near-instant posture awareness.

180+
New Product Innovations securely brought to market — our sixth consecutive year over 100, proving speed and security aren't at odds.

52
Certifications and authorizations obtained from outside auditors, validating our depth and rigor.

43
Physical security assessments completed to protect our people, data, and assets.

35+
Forums participated in globally to share intelligence and strengthen collaborative defenses.

18
Tabletop exercises simulating crisis scenarios at the executive and regional levels.

6
Consecutive years achieving 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.

State of play

Cybersecurity in 2025

Prioritization Pivot

In 2025, companies continued to see an increase in cyberattack volume, frequency, and speed. Against this backdrop, advanced teams embraced AI to expand what could be neutralized automatically, so fewer threats required human intervention. Simultaneously, the industry refined its definition of risk. While generic risk scores have always lacked nuance and context, the 2025 threat landscape made them especially misleading.

To account for this, security leaders shifted to tailored scores that were more specific to their companies' unique environments — factoring in variables such as whether a system was internet-facing, strictly access-controlled, or holding sensitive data. This allowed teams to filter out flaws with high risk scores but low practical risk to their specific company, and instead prioritize vulnerabilities that actually threatened the business.

The Evolution of Third-Party Risk

Supply chain vulnerabilities have challenged the industry for more than a decade, but in 2025, the tactic shifted. Attackers moved beyond exploiting software flaws to hijacking legitimate access. By compromising vendors and stealing their credentials, criminals effectively ”became” the partner — using authorized connections to bypass defenses unnoticed.

This evolution turned a supply chain problem into an identity crisis, requiring companies to verify trusted partners as rigorously as they do external threats.

AI Agent Governance Gap

As AI evolved from simple chatbots into powerful agents capable of connecting to internal systems to do real work, it became clear that while these tools could access sensitive data, they potentially lacked the controls to keep it safe.

This created a split in the industry. Some companies rushed in, accepting the risk of using tools they might not be able to fully monitor or stop during an emergency. Others paused adoption entirely, out of a fear of flying blind. But the most effective teams found a third way. They built their own custom safety checks to secure their data, using their existing foundational security controls, and simultaneously worked with vendors to close architectural gaps.

Credentials' Expanding Attack Surface

The identity attack surface widened dramatically in 2025, exposing both people and machines. Attackers weaponized AI to launch hyper-realistic deepfakes and phishing campaigns that routinely fooled even savvy employees, and the machine identity ecosystem grew unchecked.

As companies rushed to automate, they generated thousands of non-human credentials (like API keys) that lacked the rigorous oversight applied to humans. Attackers seized on these silent, high-access targets, proving that protecting identity now requires governing every entity that connects to the network, human or otherwise.

Our actions

Equifax Security initiatives and results in 2025

Modernized our Approach to Security Culture

Every employee and contractor recognizes that security is a critical part of their job. We reinforced this by introducing an AI-powered platform that delivers personalized, gamified training to our entire workforce.

We validated their training through more than **240,000 global phishing simulations in 2025** — 15% more than 2024 — increasing difficulty to match the threat landscape. And we expanded scorecards to include six new role-based behaviors, driving a 10% improvement against a certain behavior in just four months, showing that clear feedback moves the needle.

Demonstrating that security is a personal priority, employees used our new phishing reporting tools to flag 20,000 potential threats in just six months, surfacing nearly 1,500 confirmed malicious indicators.

Reinforced Security as a Market Differentiator

Security is a competitive differentiator that enables commercial success. We scaled our defenses to enable the secure launch of a record number of NPIs in 2025, while obtaining 52 certifications, including critical U.S. government authorizations.

We also deployed a specialized AI knowledge base that generates security questionnaire responses based solely on our official policy documentation. Early metrics show a 67% success rate on first-pass answers, far surpassing legacy solutions and allowing us to **meet customer needs with unprecedented speed.**

In 2025, a Fortune 50 telecommunications leader **publicly highlighted Equifax as the industry model** for ”doing security the right way,” citing our transparency as a key driver of their trust in us. Our commitment to transparency is a global one, with more than 4,000 users across 70 countries accessing our public security controls framework to strengthen their own defenses last year.

Unified Security and Engineering

In 2025, we **combined our Security Architecture and Technology Architecture functions,** uniting builders and defenders to drive consistent, automated solutions across the globe.

Through this shared foundation, we have fundamentally architected our systems to remove friction. By providing engineering teams with a **streamlined, automated development platform** that offers one-click deployments and seamless onboarding, we empowered them to securely **ship 50% more changes** — proving that we can accelerate technology and product innovation without compromising security.

This operational speed extended to our defenses. With better visibility, we identified, assessed, and ensured remediation of more than 3,700 critical infrastructure components — **a 164% increase in coverage** year-over-year. Despite this higher volume, we maintained an **average issue closure time of less than 24 hours**, demonstrating that when security is collective, we fix issues as fast as we find them.

Co-innovated with Vendors and Partners

Equifax continues to drive industry standards through co-innovation, a strategy where we **partner directly with our security vendors to shape product and service enhancements** that secure not only our environment but other companies' as well.

We helped our endpoint protection partner **close visibility gaps** in Linux server infrastructure, challenged our cloud provider to **develop more granular access controls** for generative AI, pushed for **critical hardware fixes**, and worked with our identity and access manager provider to **optimize infrastructure, reducing latency** to improve productivity.

This collaboration also extended beyond technology vendors to the public sector. For example, we joined 25 partners and Canadian law enforcement to help **execute over 3,000 actions against fraud networks**. We also expanded our partnership in Latin America, **working with government bodies in El Salvador and Costa Rica** to advance AI security education and shape national standardization frameworks.

Using AI to enhance security

We applied new technology to do what we've always done — only faster and with greater precision. By deploying AI as a strategic force multiplier, we upgraded our ability to not only triage and remediate threats, but also to accelerate the critical security decisions that drive business delivery.

We started using agentic AI to handle routine alerts, freeing analysts for complex threats.

Security Operations Centers (SOCs) face a universal challenge: alert fatigue, where analysts must slog through thousands of low-risk notifications.

So we engineered and piloted a specialized triage agent with a strict mandate: analyze low-fidelity alerts and only close them if they meet a rigorous ″definition of done.″

With full adoption across our global SOC scheduled for 2026, this tool added a new layer to the automation suite that accelerates issue closure while helping experts spend less time closing tickets and more time hunting sophisticated adversaries.

Impact | Auto-resolving nearly **50%** of all SOC incident tickets through automated defenses.

We drastically reduced the time it takes to test our defenses against new threats.

In the past, testing our defenses against the latest criminal tactics was a manual process. By the time a test was designed, the adversary had often moved on.

To shrink this window, we built an AI-powered engine that reads unstructured cyber threat reports and instantly converts them into actionable attack scenarios. This allows us to simulate these attacks and validate our defenses against the latest adversary tactics within days of their discovery, ensuring our shield is always calibrated to the current threat.

Impact | Moving from **threat disclosure** to **defense validation** in days, not months.

We embedded custom AI assistants to slash friction for the business.

To ensure our security processes support rapid innovation and seamless customer dialogue, we used AI to streamline two critical workflows.

First, an AI advisory assistant now helps architects analyze designs instantly, reducing security consult resolution time from 46 days to 18.

Second, an AI knowledge base accelerates customer security questionnaires by grounding answers in validated policy. This tool achieved a 67% first-pass success rate, allowing our teams to respond to customers with greater speed and accuracy.

Impact | Reducing security consult times by **61%** and accelerating sales responses.

We moved beyond finding flaws to fixing them automatically.

Traditional security tools stop at detection — alerting developers to a vulnerability and adding it to their backlog. We took this a step further by deploying AI agents to not just find problems, but also to solve them.

Using a custom AI architecture, our system analyzes container vulnerabilities and automatically writes the code fix. It then submits a ″pull request″ for the developer to review and merge. This shifts security from a gatekeeper that slows things down to a partner that cleans up code.

Impact | Handling **213,000+ findings** annually without slowing down product delivery.

Securing the business's use of AI

As our workforce and developers embraced AI to drive innovation, our priority was to ensure they could do so securely. We focused on building the necessary guardrails — from automated content safety filters to secure coding frameworks — that allowed our teams to adopt powerful new tools without exposing the enterprise to potential data leakage or unmanaged risk.

We made AI models safer for use with business data.

We designed our architecture so that we never rely solely on a model provider to protect our data. Instead, we implemented an agnostic control layer that sits between our employees and the AI.

This layer sanitizes prompts and responses, checking for sensitive data leakage or malicious injection attacks before they ever touch an AI model. This ensures that even if an external model is compromised, our data remains shielded.

Impact | Providing a **unified control layer** for prompt injection and personal data protection.

We designed the protocols that allow every employee to be an AI builder.

To scale AI safely within Equifax, we moved away from manual gatekeeping to Policy-as-Code. Our evaluation gates automatically test every new agent before production, and continuous monitoring detects if a model begins to drift or behave unpredictably.

This positions us to meet evolving AI regulations by ensuring that, for high-stakes use cases, we enforce human-in-the-loop approvals and automated kill switches with instant rollback capabilities. This framework allows us to democratize AI tools with the confidence that safety nets are always active.

Impact | Securely deploying GenAI tools to **~22,000 employees and contractors** globally.

We replaced ”shadow AI” with precision control and curated access.

We rejected the ”default on” approach of major vendors. When new features introduced potential data risks, we selectively paused them until they could meet Equifax security standards and controls.

Simultaneously, we moved from blocking innovation to guiding it. We enforced a strict deny list for high-risk external models while providing instant access to a pre-approved list of enterprise-ready tools. This ensures our developers build on a foundation of trust.

Impact | Reducing risk through **selective, compliant feature enablement.**

We implemented safe code connections for AI agents.

As AI moves from simple chatbots to autonomous agents that can edit code, the risk of an ”over-privileged” agent grows. To address this, we defined a rigid security framework for the Model Context Protocol (MCP).

By enabling developers to use remote MCP servers to access live code securely, we ensure they can leverage the latest AI assistance without giving a machine unchecked access to the entire codebase.

Impact | Operationalized **secure AI-to-code connectivity.**

Defending against AI threats

We recognized that criminals were also adopting AI-enabled tools to create highly realistic impersonations and launch faster, more complex attacks. So we recalibrated our defenses to detect and protect from these threats, ensuring our controls remained effective against a new generation of AI-enabled fraud and cyber attacks.

We successfully intercepted a deepfake attack targeting our leadership.

In 2025, the theoretical threat of AI voice cloning became a reality. Our cyber teams detected a sophisticated social engineering attack featuring a deepfake voice memo impersonating our CEO.

We didn't just stop the attack; we used it to strengthen our immunity. We instantly analyzed the adversary's linguistic patterns and deployed custom detection rules across our email gateways, effectively inoculating the organization against future AI-generated fraud attempts.

Impact | Turning a **live deepfake attempt** into a permanent defense upgrade.

We uncovered and blocked invisible attacks designed to trick AI models.

As we integrated AI, our attack simulation team discovered a novel vulnerability: adversaries could embed invisible text prompts — undetectable to the human eye — that trick AI models into delivering malware.

We successfully transitioned this discovery from a test case to a live prevention control. We implemented logic to strip these hidden commands before they reach our ecosystem, closing a loophole that many organizations haven't yet detected.

Impact | Moving from **simulated attack** to **prevention control** in record time.

We deployed adaptive defenses to catch evasive, AI-driven attacks.

Attackers are using AI to write code that constantly rewrites itself to bypass traditional filters. These ”polymorphic” attacks are designed to look different every time they strike.

In response, we deployed custom evasion logic in our endpoint defenses. Rather than looking for a specific file signature, our tools now analyze the code's behavior, allowing us to detect and block AI-generated malware regardless of how it disguises itself.

Impact | Blocking **evasive AI malware** that bypasses traditional filters.

We hardened our consumer portals against AI-driven bot swarms.

Automation allows criminals to attack at a scale humans cannot match, using ”swarms” of bots to scrape data or test stolen credentials against our consumer portals. To protect high-value targets, we deployed advanced blocking mode profiles.

These defenses identify and neutralize AI-driven tactics like ”email tumbling” (rapidly modifying a single address to bypass filters), ensuring that our data remains accessible to people, but not to bots.

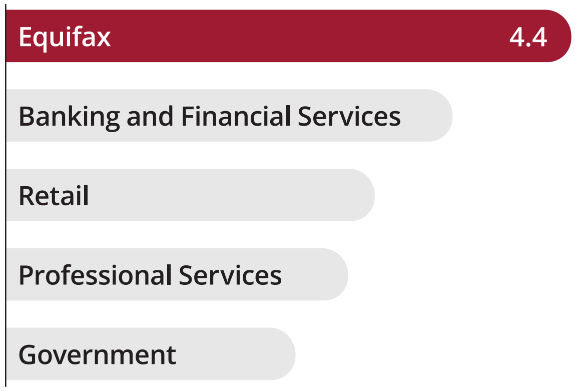
Impact | Neutralizing **sophisticated credential scraping campaigns** in real-time.

Independent benchmarking

Security Maturity

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.

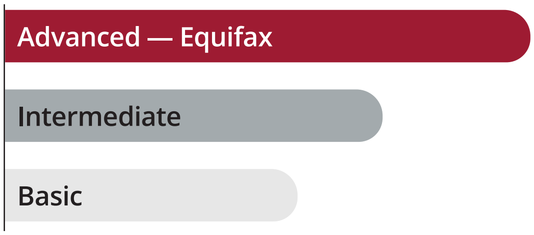
Security Maturity Score



Security Posture

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

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 Maturity?

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

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.

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.

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

Summary of results

Equifax Security in 2025

Security Posture and Maturity

- Achieved record Security Maturity rating, with a 2025 National Institute of Standards and Technology (NIST) Cybersecurity Framework score of 4.4, outperforming all major industry benchmarks for the sixth consecutive year.
- Achieved a Security Posture rating that exceeded technology industry benchmarks for a fifth consecutive year — demonstrating consistently strong security posture to customers and regulators.

Compliance

- Successfully obtained 52 certifications in 2025 with a 2% year-over-year reduction in cost per certification, and a 66% decrease from 2018.
- Streamlined compliance by launching an automated evidence portal and a new dashboard to map findings directly to specific controls — reducing the manual compliance burden.

Mergers and Acquisitions

- Achieved integration of two previous acquisitions using our repeatable, NIST based M&A framework — ensuring a more secure transition.
- Accelerated the M&A lifecycle by combining agentless API assessments with generative AI — slashing due diligence timelines from weeks to days while automating data analysis for faster, smarter integrations.

Cybersecurity

- Identified, assessed, and ensured remediation of over 3,700 critical infrastructure components, a 164% year-over-year increase, while maintaining < 24 hour average closure time — significantly reducing the organization's attack surface.
- Built and piloted a new AI triage agent which is now helping auto-resolve nearly 50% of all SOC incident tickets.
- Maintained passwordless logins for our nearly 22,000 employees and contractors globally.
- Completed migration to cloud-native access management for ~2,000 applications, improving access control and visibility.
- Deployed AI to translate unstructured threat intelligence reports into actionable simulated attack scenarios — allowing us to test our defenses against new adversary tactics within days of their discovery, not months.
- Enforced Multi-factor Authentication (MFA) for 100% of remote access, reducing unauthorized entry risks.

Physical Security and Investigations

- Completed 29 physical penetration tests, identifying continual improvement areas.
- Conducted 43 physical security assessments to secure employees, data, and assets.

Risk Management

- Established a quantitative risk engine as the authoritative source of truth for security metrics, enabling daily ingestion and prioritization of vulnerability remediation tasks.
- Performed deep-dive risk analyses on 100% of our company's critical and high-risk third parties (2,289) — driving actionable remediation plans where needed.
- Completed risk assessments on 100% of business applications (4,022) to establish a comprehensive understanding of asset risk.
- Continued to onboard key strategic accounts, including some of the largest financial institutions in the world, onto CloudControl — providing real-time visibility into the security of their Equifax products and services.

Crisis Management

- Conducted 18 tabletop exercises with company stakeholders, including:
  - CEO and Executive Team
  - Regional and Business Unit Crisis Teams
- Introduced new tabletops focused on insider threat, AI modeling, ransomware, and social engineering scenarios — equipping leaders to respond to advanced threats.
- Implemented tailored crisis plans and facilitated regional tabletop exercises in Spanish and Portuguese to ensure local team readiness.
- Integrated Crisis Management with Business Continuity and Disaster Recovery — forming a single, unified Business Resilience organization.

Security Training

- Conducted over 240,000 phishing simulations (15% year-over-year increase), continuously increasing difficulty as the threat landscape evolves.
- Re-targeted employees who have demonstrated phishing susceptibility to further educate on common threat actor techniques.
- Introduced a new threat reporting tool, driving 20,000+ reports of potential phishing from employees and contractors in just 6 months, nearly 1,500 of which were confirmed to include malicious indicators.
- Incorporated 6 new factors into employees' monthly Security Snapshots, including behaviors related to:
  - Access Certification, evaluating the timely recertification of user access, account usage and entitlement ownership.
  - Golden Image Utilization, measuring if engineers are using standardized golden images for environments.
  - Issue Governance, measuring timeliness of closing open security issues.

Customer Engagement

- Completed 2,599 client questionnaires, with an average completion time of 1.86 days, providing rapid security assurance to external parties.
- Completed 1,149 evidence requests at the request of Equifax customers to ensure compliance.
- Securely brought 180+ NPIs to market — our sixth consecutive year over 100.

Privacy

- Implemented a new tool for email data loss prevention (DLP), providing greater compatibility with our existing toolset, more robust analytics and enhanced global compliance.
- Obtained re-certification to Data Privacy Framework (DPF) for the second year, enabling secure EU/UK to U.S. data transfers.
- Launched a new consent management platform globally to respect website visitor choices.

Fraud

- Finalized the Global Fraud Monitoring Strategy and standardized fraudulent account blocking into a single cloud platform, unifying processes across business units.
- Blocked over 3,700 suspicious devices and 2,900 suspicious IPs through fraud investigations.
- Fraud incidents involving exposure of sensitive data dropped by 18% year-over-year, highlighting our ability to stop suspicious activity before it escalates.
- Established a new fraud team in India, providing expanded global fraud coverage and capacity across multiple time zones.

Secure Software Development

- Improved Infrastructure-as-Code (IaC) adoption by 52%, leveraging standardized code blocks to ensure alignment with Equifax configuration standards and eliminate manual misconfigurations.
- Released an AI-powered personal assistant for Security Advisory Services (SAS) workflows that reduced the average time-to-resolution for consults by 61% and cut initial escalation requests by 56%.
- Developed custom AI architecture to analyze container vulnerabilities and automatically write the code fix, simplifying the workflow of resolving 213,000+ findings annually.
- Launched the Automated Certificate Management Toolkit to automate the renewal of application TLS certificates (the digital credentials that encrypt data in transit). This tool tracks due dates and upgrades and tests certificates without manual intervention.

Our priorities in 2026

Securing Every Identity: Human and Machine

By eliminating credentials for our entire workforce, we've proven that passwordless is possible. In 2026, we're scaling that revolution. We'll begin rolling out an option for passwordless logins to our B2B customers, neutralizing credential stuffing attacks while removing friction for our partners.

Simultaneously, we're targeting the silent majority of identities: non-human accounts. As our AI agents and APIs multiply, we're applying the same rigorous verification to machines that we do to people, ensuring that a bot cannot be used as a backdoor.

Scaling Our Agentic Governance

In 2025, we built the protocols to secure our first generation of AI agents. In 2026, we're industrializing that safety net. We're expanding our Policy-as-Code framework to cover every corner of the enterprise, automating the testing of thousands of agents for safety, drift, and strict data privacy. This governance-by-design approach ensures we stay ahead of the complex AI regulatory landscape.

By scaling these automated guardrails, we'll enable Equifax to move from piloting agentic workflows to running them as a standard, high-volume business engine — without ever compromising our security and control.

Evolving Contextual Risk

When it comes to analyzing security risk, we are adept at filtering out noise and factoring in context, including asset value, internet exposure, and compensating controls. Now, we're changing how we see the signal.

In 2026, we're overhauling how security risk is visualized, turning complex calculations into a high-fidelity map of business exposure. We're also standardizing assessments for edge cases and validating our asset inventory to ensure our picture is complete. This evolution converts abstract risk data into clear, undeniable business signals, making the next right move obvious to every decision maker.