



FY25 Sustainability Update



Table of Contents

At CrowdStrike, our mission is to stop breaches.

We are passionate about protecting our future and keeping the world safe. We bring that same passion to helping our people, communities, and planet thrive — today and tomorrow. With this FY25 Sustainability Update, we are proudly spotlighting how CrowdStrikers are making a positive impact worldwide.



Overview

- 03 About This Update
- 04 Letter From George Kurtz
- 05 FY25 Sustainability Highlights
- 06 About CrowdStrike
- 07 Awards and Recognition
- 08 Sustainability Approach

Security and Resilience

- 11 The CrowdStrike Falcon Platform
- 12 Risk Management
- 13 Cybersecurity Risk Management
- 14 Data Privacy
- 16 Information Security
- 17 Responsible Use of AI

Governance

- 19 Corporate Governance
- 20 Ethics and Compliance
- 22 Stakeholder Engagement
- 23 Public Policy

Social

- 25 Our People
 - 26 Attracting and Retaining Talent
 - 27 Listening and Learning
 - 28 Connection and Collaboration
 - 29 Benefits and Compensation
 - 30 Employee Well-being
 - 31 Learning and Development
 - 32 Protecting Workers' Rights
- 33 Our Communities

Environmental

- 38 Climate Risk and Opportunity
- 39 GHG Emissions and Energy Consumption
- 42 CrowdStrike Data Centers
- 43 CrowdStrike Offices
- 44 CrowdStrike Operations
- 45 Employee Action
- 46 Sustainability Policies
- 47 Appendix: TCFD Index

About This Update.

Date: October 27, 2025

As used in this report, references to CrowdStrike, the “Company,” “we” and “our” refer to CrowdStrike Holdings, Inc. and its subsidiaries.

Reporting Period

This Sustainability Update provides an overview of CrowdStrike’s environmental efforts, social impact, and corporate governance practices for the fiscal year 2025 (February 1, 2024, to January 31, 2025).

Reporting Scope and Frameworks

This is a voluntary update to offer our stakeholders insight into our sustainability strategy and performance.

In FY25, CrowdStrike acquired Flow Security and Adaptive Shield, and all GHG emissions and energy consumption are included within our GHG emissions and energy consumption footprint calculations.

Forward-Looking Statements

This report contains forward-looking statements that involve risks, uncertainties, and assumptions, including statements regarding CrowdStrike’s business strategy, plans, goals and future operational and financial performance, sustainability strategies, initiatives and commitments; climate risk

assessment, management and mitigation measures; and long-term outlook. Forward-looking statements are based on current expectations and assumptions as of the date of this report and are subject to known and unknown risks and uncertainties that may cause actual results to differ materially from those expressed or implied by such statements.

These risks include, but are not limited to, risks associated with CrowdStrike’s ability to achieve its sustainability goals and implement related programs successfully; the potential impact of evolving regulatory frameworks, stakeholder expectations, and disclosure requirements; risks associated with managing rapid growth; CrowdStrike’s ability to identify and effectively address execution challenges; risks associated with new products and subscription and support offerings; CrowdStrike’s ability to respond to an intensely competitive market; industry trends; rapidly evolving technological developments in the market for security products and subscription and support offerings; the ability to retain and attract customers and talent; integration risks related to acquisitions; and general market, political, economic, and business conditions, including those related to a deterioration in macroeconomic conditions, inflation, geopolitical uncertainty and conflicts, public health crises, and volatility in the banking and financial services sector.

Additional information regarding these and other risks is included in CrowdStrike’s filings with the U.S. Securities and Exchange Commission (SEC), including under the captions “Risk Factors” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations” in CrowdStrike’s most recently filed Annual Report on Form 10-K, most recently filed Quarterly Report on Form 10-Q, and other SEC filings.

CrowdStrike undertakes no obligation to update any forward-looking statements contained in this report to reflect new information, future events, or otherwise, except as required by applicable law.

This Sustainability Update contains human capital measures or objectives that may be different from, or are in addition to, the human capital measures or objectives that CrowdStrike is required to disclose in its SEC filings. For a discussion on human capital measures or objectives that CrowdStrike focuses on in managing its business, please see the “Human Capital Resources” section in our most recent Annual Report on Form 10-K.



We engaged an external third party to perform limited assurance procedures over certain metrics disclosed in CrowdStrike’s FY25 Sustainability Update for the year ended Jan. 31, 2025. The external third-party report is available [here](#).

Letter From George Kurtz.

Our mission since our founding is clear: to stop breaches. This mission has never been more urgent. We live in the AI era, where adversaries are weaponizing AI to accelerate attacks, expand their reach, and exploit every vulnerability in our digital world. The stakes are high. What we protect is not just data or infrastructure, but the security of economies, communities, and the trust that underpins modern life.

Delivering on this mission demands speed, innovation, and resilience. A sustainable CrowdStrike is one that is always ready, able to withstand challenges, adapt to change, and continue creating value for those who depend on us.

Resilience starts with our people and our platform. We invest in the industry's best talent and the innovation that makes the Falcon platform the most trusted cybersecurity platform in the world. Our 10,000+ CrowdStrikers extend this mission globally, helping to build a future where security is the foundation for thriving communities, strong economies, and healthy ecosystems. Without security, none of these are possible.

This FY25 Sustainability Update reflects this conviction. It outlines the steps we are taking to demonstrate resilience across our culture, our operations, and our strategy.

Since our founding in 2011, we've built a company rooted in our mission and values. Some of our FY25 milestones, such as being Great Place to Work-certified in nine countries, show how we've scaled culture with growth. Others, such as calculating our FY25 greenhouse gas emissions as a baseline for measuring progress, demonstrate our discipline in preparing for the future.

We apply the same rapid innovation that defines our security solutions to developing new sustainability efforts for our company. Highlights include establishing an AI leadership team, completing our first Climate Risk Scenario Analysis, and expanding our partnership with the Center for Infrastructure Assurance and Security, providing cybersecurity education to more than 100,000 students across 28 countries.

Our focus remains clear: Stop adversaries, demonstrate resilience, and prepare the next generation of defenders.

We know these challenges are bigger than any one company. Through focus and collaboration with our stakeholders, we will continue to build a secure and sustainable future, not just for CrowdStrike, but for generations to come.

George Kurtz
CEO and Founder

George Kurtz

10,000+

Our 10,000+ CrowdStrikers extend this mission globally, helping to build a future where security is the foundation for thriving communities, strong economies, and healthy ecosystems.



FY25 Sustainability Highlights.

Security & Resilience

- 6 trillion events processed weekly
- Launched internal generative AI solution

6 trillion

Environment

- Calculated our FY25 Scope 1 and Scope 2 greenhouse gas emissions
- 60% of our buildings are LEED- or ENERGY STAR-certified
- Initiated a Climate Risk Scenario Analysis



60%



Social

- Great Place to Work-certified in 9 countries
- 96% of CrowdStrikers agreed this is a great place to work*
- 100,000 students reached by the Center for Infrastructure Assurance and Security's (CIAS) cybersecurity education through CrowdStrike's support**

100,000

Governance

- Launched "Ethics & Compliance Week" employee awareness initiative
- Engaged with policymakers, government agencies, and industry stakeholders to advance cybersecurity policy and protect organizations from cyber threats

* 2024 Great Place to Work survey
** Center for Infrastructure Assurance and Security

About CrowdStrike.

One platform. Every industry. Superior protection.

CrowdStrike has a singular mission: We stop breaches. As a global cybersecurity leader, we've redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity, and data.

Powered by the CrowdStrike® Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

Our Core Values

We are Fanatical About the Customer and Relentlessly Focused on Innovation, and we believe that our Limitless Passion Creates Unlimited Potential for every CrowdStriker.



74,000+

CrowdStrike is trusted by more than 74,000 organizations, including our end customers and those of our managed security service providers (MSSPs).

CrowdStrike (NASDAQ: CRWD):

Founded:
2011

Principal Executive Offices:
Austin, Texas

FY25 Revenue:
\$3.95 billion (29% YOY increase)

Global Employees:
10,000+

Including our end customers and those of our managed security service providers, CrowdStrike is trusted by more than 74,000 organizations

CrowdStrike protects:

314
of the Fortune 500

8 out of the top 10
financial services firms

8 out of the top 10
manufacturers

564
of the Fortune 1000

9 out of the top 10
food & beverage companies

8 out of the top 10
auto companies

42
of the 50 U.S. states

8 out of the top 10
healthcare companies

8 out of the top 10
technology firms

Awards and Recognition.



CrowdStrike is dedicated to creating the industry's best products and place to work. We are proud of the recognition these efforts received in FY25. Below are just a few key honors — visit our [newsroom](#) for more.

S&P 500®

Listed on the S&P 500



Fortune 100 Best Companies to Work For® 2024



Fortune Best Workplaces in Technology 2024



Great Place to Work-certified in nine countries



AWS 2024 Global Security Partner of the Year



Leader, 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (fifth consecutive year)



Frost & Sullivan’s Company of the Year in the Global Managed Detection and Response (MDR) Market Industry



Leader, 2024 GigaOm Radar Report for Container Security



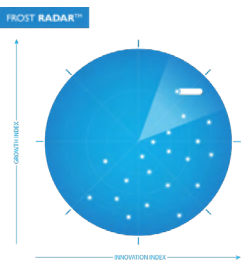
Leader and Outperformer, 2024 GigaOm Radar Report for Ransomware Prevention



Customers’ Choice, 2024 Gartner Peer Insights™ “Voice of the Customer” MDR Report



Overall Leader, KuppingerCole’s 2024 Leadership Compass for MDR



Leader, 2024 Frost Radar™: Cloud-Native Application Protection Platforms (third consecutive year)

In January 2025, CrowdStrike marked our inaugural participation in the World Economic Forum’s Annual Meeting in Davos, where cybersecurity has emerged as a critical agenda item for world leaders. As a speaker on two panels, CEO George Kurtz underscored the critical role of cybersecurity in shaping national and organizational resilience strategies.



Sustainability Approach.

Protecting our future.

Our sustainability strategy focuses on protecting what matters most and making a lasting, positive impact on our world. Following our mission to stop breaches, our impact starts with protecting the security and resilience of our company, our customers, and the people they serve. We hire the industry's best people to fulfill this mission and cultivate a positive, rewarding work environment for all CrowdStrikers.

We help contribute to protecting our shared home — planet Earth — by reducing the environmental impact of our cloud platform and operations. We amplify our impact further through dedicated social impact initiatives that protect, educate, and uplift communities. We do this while leading with our core values and maintaining strong corporate governance and ethical business practices.

Our Impact Areas

We organize our sustainability impact areas based on how CrowdStrike's influence flows out into the world. We maintain a foundation of security and resilience, govern with integrity, and hire and develop the best people based on merit. Together, our global team cares for our communities and the planet.

Security and Resilience	Governance	Social	Environmental
<ul style="list-style-type: none">• Risk Management• Cybersecurity• Responsible Use of AI	<ul style="list-style-type: none">• Ethics & Compliance• Stakeholder Engagement	<ul style="list-style-type: none">• Our People• Our Communities	<ul style="list-style-type: none">• Climate Change Mitigation & Adaptation• Energy Use

Associations

As an active member of Business for Social Responsibility (BSR) and the Association of Corporate Citizenship Professionals, CrowdStrike learns from and shares best practices with sustainability and social impact leaders worldwide.



Best

We hire the industry's best people to fulfill our mission and cultivate a positive, rewarding work environment for all CrowdStrikers.

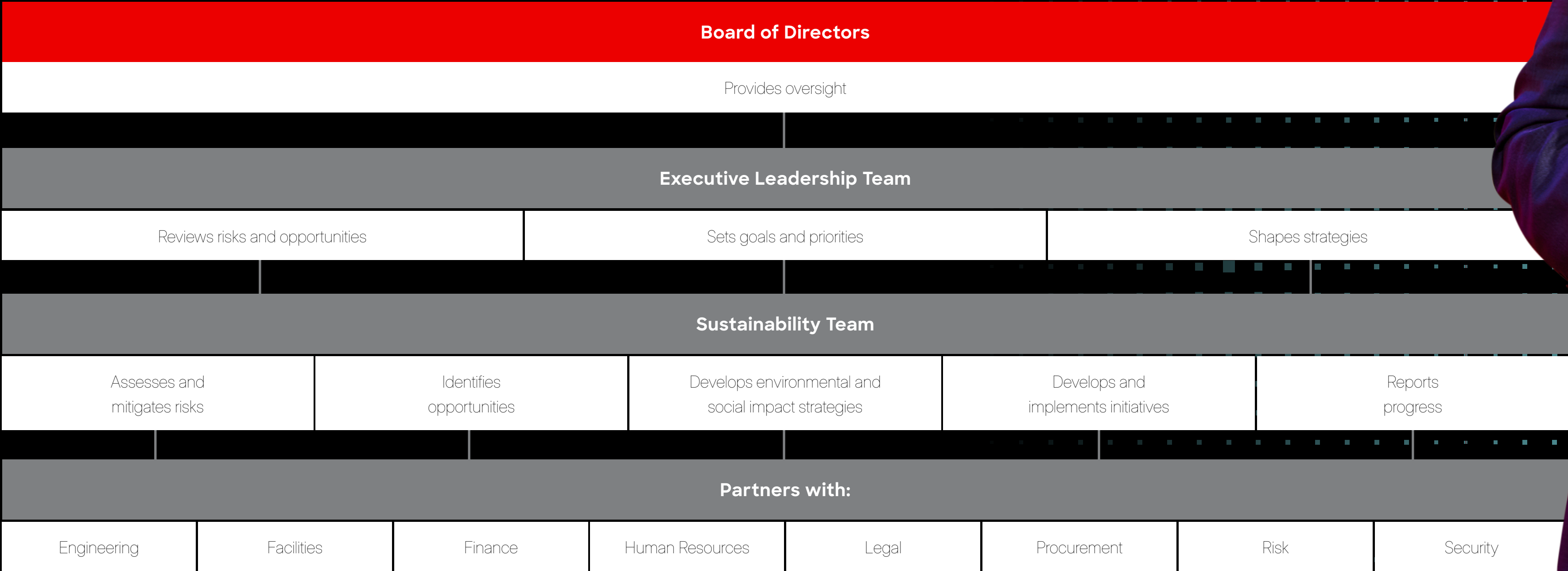


Sustainability Approach.

Sustainability Governance

Sustainability oversight and management is a cross-company effort at CrowdStrike. Our dedicated sustainability team spearheads environmental stewardship, social impact, and reporting, partnering with teams across CrowdStrike. Our legal team supports and refines our corporate governance policies and practices, our security team embeds cybersecurity into every aspect of our business, and our human resources team drives our workforce initiatives.

CrowdStrike's executive leadership team sets priorities and guides strategic direction, with oversight from our board of directors. Our global team of CrowdStrikers — alongside our partners and customers — uses their passion and innovation to make positive change daily.



Michael Sentonas
President

Security and Resilience.

Creating lasting value.

Securing the world's most critical organizations demands reliability. We maintain robust information security and privacy practices as the foundation of everything we do — because our customers' security starts with our own. Through proactive risk management and continuous assessment and enhancement of our critical capabilities, our customers have the partner they need to navigate today's evolving threats and emerging technologies.

Our approach to security and resilience is designed to create lasting value, supporting the long-term sustainability of both CrowdStrike and our customers. By fostering a secure digital ecosystem, we contribute to the overall resilience of the global economy, enabling organizations to thrive in an increasingly interconnected world.

In this section

- 11 The CrowdStrike Falcon Platform
- 12 Risk Management
- 13 Cybersecurity Risk Management
- 14 Data Privacy
- 16 Information Security
- 17 Responsible Use of AI

A portrait of Justin Acquaro, Chief Information Officer, wearing a blue checkered blazer over a light blue shirt. He is seated with his hands clasped in front of him. The background features bold, diagonal red and black stripes.

Justin Acquaro
Chief Information Officer

The CrowdStrike Falcon Platform.

The cybersecurity platform for the AI era.

CrowdStrike's [Falcon platform](#) is foundational to our mission of stopping breaches. With the Falcon platform, we created the first multi-tenant, cloud-native, intelligent security platform capable of protecting workloads across on-premises, virtualized, and cloud environments, including desktops, laptops, servers, virtual machines, cloud workloads, cloud containers, and mobile and internet of things (IoT) devices.

We offer 32 cloud modules on the Falcon platform via a software as a service (SaaS) model, spanning multiple large security markets, such as corporate endpoint and cloud workload security, managed security services, IT operations management, identity protection, next-gen security information and event management (SIEM), threat intelligence, data protection, and AI-powered workflow automation, including securing generative AI workloads.

By consolidating multiple cybersecurity functions into a single, unified platform, the Falcon platform simplifies operations, reduces costs, and improves overall security effectiveness for our customers. This approach protects individual organizations and contributes to the overall resilience of the digital ecosystem, helping to create a more secure future for businesses, governments, and individuals alike.



32

We offer 32 cloud modules on the Falcon platform via a SaaS model, spanning multiple large security markets.



Unified platform. One sensor. Complete protection.

Risk Management.



Outmaneuvering risk at every turn

CrowdStrike actively hunts threats in a landscape of constant risk. Effective risk management isn't just a good business practice — it's essential to our credibility and capability. By excelling at risk management, we strengthen our own defenses, enhance our ability to innovate, and sharpen our capacity to protect our customers. Our comprehensive approach, aligned with the Committee of Sponsoring Organizations (COSO) [Enterprise Risk Management Framework](#), prepares us for both current and future challenges.



Risk Assessment and Monitoring

Our risk evaluation process is a collaborative effort. To create clear communication across CrowdStrike, we use a common risk language. Our specialized risk teams work with frontline staff to assess the likelihood and potential impact of various risks. We consider both operational risks that could disrupt our daily activities and strategic risks that might affect our long-term goals. These specialized teams report their findings to our Enterprise Risk Management (ERM) team, which tracks risks and shares insights with CrowdStrike's executive leadership and our board's audit committee, promoting top-level awareness and oversight of our risk landscape.



Continuous Improvement

We take a forward-thinking, continuous improvement approach to our risk management practices to maximize our resilience. We regularly review and update our processes, incorporating feedback from both specialized and frontline teams. This helps us stay ahead of emerging threats and align with industry best practices. In the past year, we've particularly focused on managing risks associated with our rapid growth.

Tiered Risk Management Strategy

Our ERM team sets CrowdStrike's overall risk management standards and maintains a company-wide view of risks.



Specialized risk teams provide guidance and oversight, working closely with frontline teams.



Frontline teams handle day-to-day risks in their work.

See CrowdStrike's [Proxy Statement](#) for its June 2025 annual stockholder meeting for a discussion of the role of CrowdStrike's board in risk oversight.



Cybersecurity Risk Management.

Setting the global security benchmark.

We are passionate about cybersecurity risk management, and it is an integral part of CrowdStrike's overall enterprise risk management program.

Program Framework

Our cybersecurity risk management program, which includes data privacy, product security, and information security, is designed to align with our industry's best practices. Our program provides a framework for identifying, monitoring, evaluating, and responding to cybersecurity threats and incidents, including those associated with our use of software, applications, services, and cloud infrastructure developed or provided by third-party vendors and service providers.

Our cybersecurity team is responsible for assessing our cybersecurity risk management program and our incident response plan. We regularly test this plan through tabletop exercises and test our security protocols through additional techniques, such as penetration testing.

We review or update our cybersecurity policies, standards, and procedures annually, or more frequently as needed, to account for changes in the threat landscape as well as in response to legal and regulatory developments.

Governance and Oversight

CrowdStrike's board of directors has oversight responsibility for our overall ERM and has delegated cybersecurity risk management oversight to the audit committee. The audit committee reviews with management:

- The policies, processes, and procedures designed to identify, monitor, evaluate, and respond to cybersecurity risks and issues
- Steps to mitigate or remediate cybersecurity risks, issues, threats, and incidents
- Our cybersecurity policies, processes, and procedures

Management and Implementation

Our cybersecurity programs are under the direction of CrowdStrike's chief information security officer (CISO). Our CISO and dedicated personnel are certified and experienced information systems security professionals and information security managers with many years of experience across a variety of technology subspecialties.

The CISO runs a monthly Cybersecurity Steering Committee where high level risks and issues get escalated for visibility, requesting a solution or decision-making.

A cross-functional incident response team, composed of representatives from information technology, information security, product security, engineering, privacy,

and legal, is responsible for the monitoring and disposition of potential occurrences such as data breaches, intrusions, and other security incidents and implementing our detailed incident response plan.

Adversary:
SCATTERED SPIDER



Data Privacy.

Maintaining trust through protection.

CrowdStrike's commitment to privacy is rooted in principle and reinforced through action. Our Global Privacy Compliance Program is a company-wide framework designed so that privacy is treated not only as a legal obligation but as a foundational component of trust, innovation, and ethical responsibility.

Grounded in Core Principles

Inspired by leading data privacy standards, including the OECD Privacy Guidelines, the Fair Information Practice Principles (FIPPs), the GDPR, and the APEC Privacy Framework, we operationalize privacy through a globally recognized set of principles:

- Fairness and Transparency
- Appropriateness and Use Limitation
- Data Retention
- Confidentiality and Integrity
- Data Quality
- Individual Privacy Rights
- Accountability

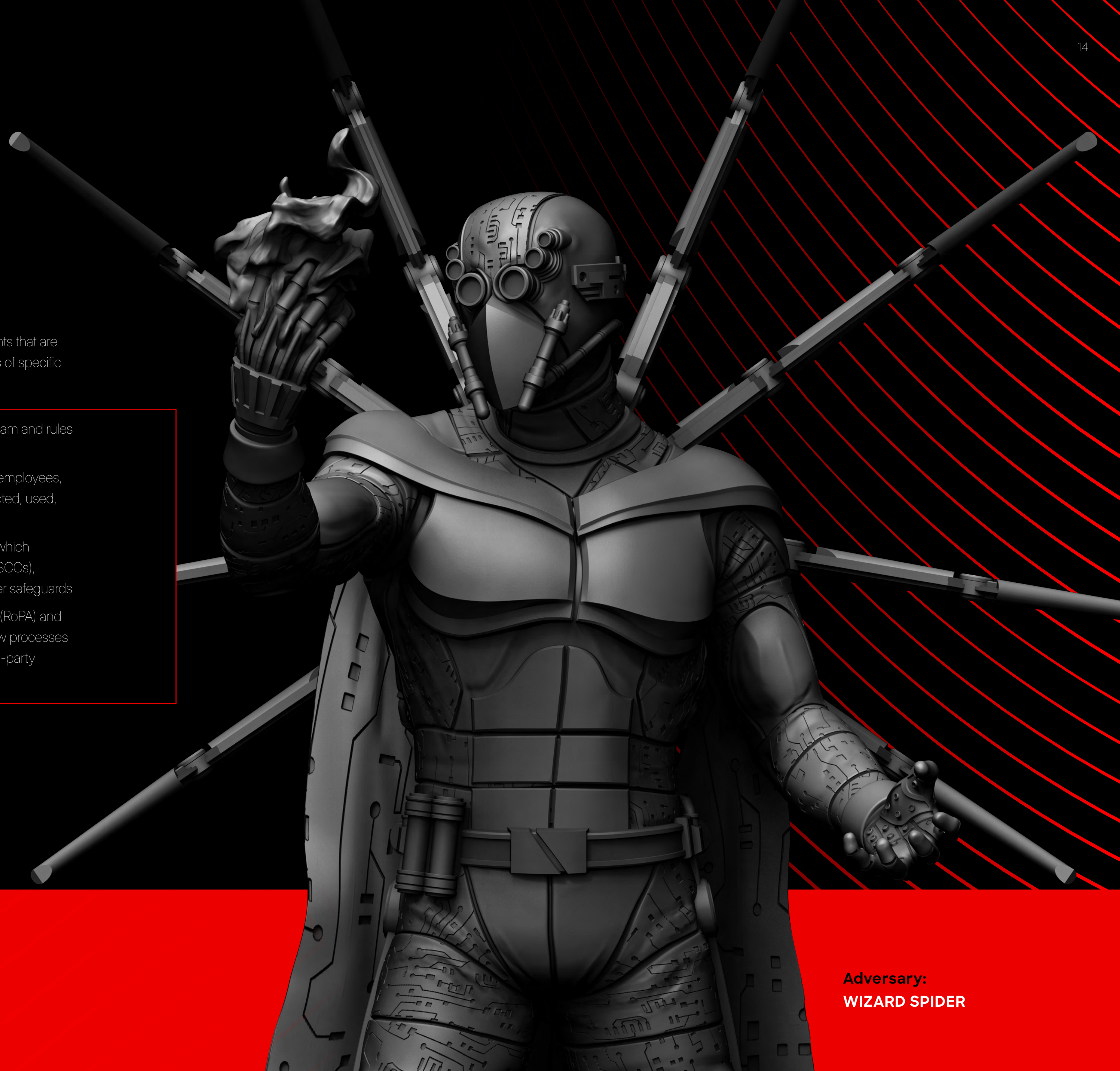
Notices, Agreements, and Policies

We formalize our privacy commitments through comprehensive policies, notices, and agreements that are globally applicable and responsive to the needs of specific jurisdictions. These include:

- Internal policies that govern our privacy program and rules for our business
- Public-facing privacy notices for customers, employees, and partners that articulate how data is collected, used, and protected
- A robust Global Data Protection Agreement, which incorporates Standard Contractual Clauses (SCCs), subprocessor transparency, and cross-border safeguards
- A centralized Record of Processing Activities (RoPA) and workflow systems, including formalized review processes for individual privacy rights requests and third-party vendor reviews

Our privacy obligations are not static — they evolve in lockstep with global regulations, and our documentation life cycle is actively maintained, version-controlled, and reviewed.

**Adversary:
WIZARD SPIDER**



Data Privacy.

Communicating Privacy Across the Organization and Beyond

CrowdStrike takes a proactive and transparent approach to communicating its privacy standards internally and externally:

- Internal teams are provided with jurisdiction-specific and use case-specific guidance through centralized repositories and on-demand consultations.
- Externally, we maintain customer-facing white papers, cross-border data transfer FAQs, and regulatory response templates, all publicly accessible via our Trust Center and Falcon dashboards.
- The privacy team collaborates with departments throughout the business to align on key priorities and embed core privacy principles in our offerings.

Training and Cultural Integration

Privacy is part of our culture. Our employees receive:

- Mandatory onboarding and annual privacy training, tailored as appropriate by function and jurisdiction.
- Professional development support for specialized positions, including internal Certified Information Privacy Professional (CIPP) training tracks to deepen fluency in privacy.

Demonstrated Compliance and Third-Party Certifications

We demonstrate accountability with our core privacy principles through internal controls as well as third-party certification and verification. CrowdStrike holds certifications in or participates in:

- EU-U.S., U.K., and Swiss Data Privacy Frameworks (DPFs)
- APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) frameworks
- Global Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) frameworks
- Designated data protection officer (DPO) registrations in specific jurisdictions around the globe
- Ongoing tracking and implementation guidance aligned with emerging regulations

Our privacy team also plays a strategic role on internal governance bodies such as the AI Governance Committee (launching in FY26), Enterprise Risk Committee, and Insider Risk Committee, integrating privacy equities into broader risk management. Privacy leadership reports directly to CrowdStrike's president and provides annual updates to the board of directors' audit committee.



Information Security.

CrowdStrike's information security function works to implement cutting-edge technologies and processes that meet our security objectives. Our comprehensive program creates a robust protection framework demanded by today's risk landscape and legal standards.

We have implemented state-of-the-art security controls based on the CSA Cloud Controls Matrix (CCM) and additional frameworks like International Organization for Standardization (ISO) 27001, ISO 27002, PCI, and National Institute of Standards and Technology (NIST) 800-53. Our program is regularly reviewed by senior management as part of the company's ERM process. The program consists of various layers of technical and administrative controls to protect the confidentiality and integrity of customer data.

We maintain a comprehensive set of information security certifications, including:

- System and Organization Controls 2 (SOC 2), which validates our controls for security, availability, processing integrity, confidentiality, and privacy
- ISO 27001, the leading international standard for information security management systems
- Federal Risk and Authorization Management Program (FedRAMP) High Authorization, the U.S. government's rigorous security assessment framework for cloud services
- United Kingdom Cyber Essentials certification
- The Falcon platform attains Security, Trust, Assurance, and Risk (STAR) Level 1 and STAR Level 2 within the Cloud Security Alliance's STAR Registry
- CrowdStrike publishes a PCI Data Security Standard (PCI DSS) Attestation of Compliance annually after thoroughly assessing and validating our compliance with all 12 control requirements

Our data centers are:

- Certified under ISO/IEC 27001:2022 and the German Federal Cybersecurity Agency (BSI) Cloud Computing Compliance Criteria Catalog (C5:2022)
- Certified under the Spanish National Cryptologic Center (CCN) STIC Products and Services Catalog (CPSTIC) at the "high" level
- Granted Impact Level 5 (IL5) authorization from the U.S. Department of Defense (DoD)

CrowdStrike also achieved certification in the Australian Infosec Registered Assessors Program (IRAP) and the highest level of the Trusted Information Security Assessment Exchange (TISAX) registration (AL3) in Europe. We continue to expand our government certifications for the Falcon platform and provide global customers with the best security platform to stop breaches.

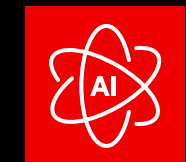


Auditing

CrowdStrike assesses information security risks through an internally designed standard that draws from the NIST Risk Management Framework (RMF), NIST SP 800-30 Rev 1, ISO/IEC 27001:2022, and ISO 31000:2018 and aligns with the Committee of Sponsoring Organizations (COSO) ERM.

Our commercial portfolio undergoes annual external audits against the SOC 2, ISO, and CSA STAR frameworks. We also run a PCI self-assessment and a voluntary product assessment test (VPAT), which is focused on both security and accessibility. Our government environments are evaluated at least twice annually.

Responsible Use of AI.



Advancing security through AI innovation.

As cybercriminals increasingly leverage AI to enhance their capabilities, AI has become both a critical threat vector and a powerful tool for cyber defense. AI-powered systems can detect and respond to threats faster and more accurately than traditional methods, making them essential in our defense against sophisticated cyberattacks and data breaches. CrowdStrike incorporates novel uses of AI technologies, including generative and agentic AI, into its products and operations, such as the Falcon platform. We recognize that we must approach the deployment of AI technology with careful consideration for security, privacy, and responsible development practices. We track emerging laws and regulations governing AI while following development practices to protect customers from negative impacts.

Internal AI Governance and Education

Our cross-functional AI leadership team guides the responsible use of AI technologies across CrowdStrike, and plans to launch an internal AI Governance Committee in FY26. This committee will provide strategic oversight, risk management, and policy direction to promote the development, deployment, and use of our AI systems in a responsible, secure, and compliant manner. The goal is to keep CrowdStrike's application and use of AI aligned with business goals, regulatory requirements, responsible use principles, and security and compliance obligations.

We have established guidelines for employees' use of generative AI, with protocols for handling sensitive, proprietary, and confidential data. In FY25, we developed an internal generative AI solution with defined use cases to support security and compliance. We use real-time messaging platforms to facilitate knowledge sharing among CrowdStrikers, and we publish an internal quarterly AI newsletter covering technological developments, regulatory updates, and policy changes.



Charlotte AI

Secure AI Development

We protect AI itself through rigorous data operations and continuous model refinement via our adversarial pipeline. We also embrace privacy-by-design and secure-by-design principles throughout our AI development life cycle, from the training data that powers our models to the queries used to automate productivity. This enables us to leverage AI for advanced threat detection while protecting customers against data breaches that threaten privacy.

Using AI to Protect Customers

We offer AI Red Team Services to help organizations assess the security of their own AI implementations. As cyber threat actors deploy increasingly sophisticated "dark AI" attacks, CrowdStrike's AI approach delivers:

- Advanced Threat Detection: AI-powered indicators of attack identify threats before they materialize
- Rapid Response: AI-mediated threat response significantly reduces critical response time

- Enhanced Threat Hunting: Combining human expertise with AI's data processing capabilities enhances threat hunting
- Democratized Security: CrowdStrike® Charlotte AI™ transforms the analyst experience through natural language interfaces

Leading in Responsible AI

CrowdStrike maintains certifications across global privacy frameworks (EU-U.S. DPF, U.K. Extension, Swiss-U.S. DPF, APEC CBPR/PRP) and actively shapes AI's future as a founding member of the NIST AI Safety Institute Consortium.

Governance

Leading with integrity.

The world's leading companies and organizations trust CrowdStrike to keep them safe. We take this responsibility very seriously, and we retain the trust of our customers and other stakeholders by backing our solutions with strong governance and ethical business practices. This commitment to leading with integrity extends throughout our organization, from board oversight to daily operations, maintaining high standards of corporate conduct while driving innovation and sustainable growth in service of our mission.

Our dedication to doing what's right extends beyond business practices to encompass how we show up in the world — extending our mission to support our people, our communities and our planet. Through this values-driven approach, CrowdStrike remains a trusted partner and a force for positive change.

[Explore Governance at CrowdStrike](#)

In this section

- 19 Corporate Governance
- 20 Ethics and Compliance
- 22 Stakeholder Engagement
- 23 Public Policy



Cathleen Anderson
Chief Legal Officer

Corporate Governance.

Expert oversight of our critical mission.

Strong corporate governance is fundamental to CrowdStrike's long-term success and its ability to create value for stakeholders. It takes skills and experience to fully understand the potential damage a breach can do. CrowdStrike's [Board of Directors](#) brings together deep expertise in cybersecurity, technology, finance, and operations to advance our mission through a culture of integrity and accountability. Their experience and perspective strengthen our strategic planning and risk management, driving innovation and sustainable growth at CrowdStrike.

CrowdStrike Board Committees

The board carries out its oversight responsibilities both directly and through its [standing committees](#), each of which operates under a written charter that clearly defines its roles and responsibilities. The audit and compensation committees also prepare committee reports for inclusion in CrowdStrike's annual proxy statement, as required by the SEC.

Audit Committee	Compensation Committee	Nominating & Corporate Governance Committee
<div><ul style="list-style-type: none">• Assist the board in its oversight of:<ul style="list-style-type: none">- The integrity of the Company's financial statements and internal controls- The qualifications, independence, and performance of the Company's independent auditor- The performance of the Company's internal audit function- The Company's compliance with legal and regulatory requirements• Prepare the Committee report that the SEC rules require to be included in the Company's annual proxy statement• Discuss with management, and as applicable, the independent auditor the Company's disclosure controls and procedures over environmental and sustainability reporting data and disclosures, and any assurance being provided by the independent auditor or other third parties with respect to such data and disclosures</div>	<div><ul style="list-style-type: none">• Establish and periodically review the Company's overall compensation strategy• Oversee and evaluate the Company's compensation and benefits policies generally, including matters regarding human capital resources• Review and assess risks arising from the Company's employee compensation policies and practices• Review and approve the compensation of the Company's executive officers• Review the Company's management succession planning• Review and make recommendations to the board regarding the compensation and benefits policies for the Company's directors• Prepare the committee report required by SEC rules to be included in the Company's annual proxy statement or Form 10-K</div>	<div><ul style="list-style-type: none">• Review and evaluate the size, composition, function and duties of the board• Recommend criteria for the selection of candidates to the board and its committees• Recommend to the board director nominees for election• Recommend directors for appointment to board committees• Make recommendations to the Board as to determinations of director independence• Oversee the evaluation of the board and its committees• Develop and recommend to the board the Corporate Governance Guidelines and Code of Business Conduct and Ethics for the Company and oversee compliance with such Guidelines and Code• Periodically review CrowdStrike's sustainability policies, programs, and progress to support the sustainable growth of the business</div>

Ethics and Compliance.

We uphold high standards.

Our ethics and compliance program promotes business conduct consistent with the highest standards of honesty, fairness, and accountability. Through clear policies, regular training, and effective oversight, we maintain comprehensive frameworks that promote ethical decision-making and regulatory compliance across our global operations. Our program emphasizes transparent communication and consistent standards for all employees, partners, and stakeholders.

Ethics and Compliance Oversight

Our ethics and legal compliance team leads our ethics and compliance program. The team provides regular updates to CrowdStrike's audit committee, executive team, and external auditors, providing appropriate oversight of program activities and outcomes.

Policies and Standards

Our ethics and compliance framework is built on several foundational policies that establish clear expectations for employee conduct and business operations. These policies undergo regular review and, where required, board approval.

Code of Ethics and Business Conduct:	Anti-bribery and Corruption Policy:	Business Partner Standards:	Rules of Engagement for Commercial Transactions:	Global Sanctions Policy:	Whistleblower Policy:
Serves as our central policy establishing fundamental standards for ethical behavior. All employees acknowledge the Code of Ethics and Business Conduct upon hiring and annually through our training program. The Code of Ethics and Business Conduct references our other key compliance policies and provides core guidance for business conduct across the organization. The nominating and corporate governance committee of CrowdStrike's board of directors is responsible for reviewing and updating the Code of Ethics and Business Conduct as appropriate.	Outlines our zero-tolerance approach to bribery and corruption. The policy provides guidelines for third-party interactions, partner incentive programs, and gifts, meals, entertainment, and travel.	Extends our ethical requirements to partners, supporting consistent compliance practices throughout our ecosystem. These Business Partner Standards mirror key elements of our internal Code of Ethics and Business Conduct and define compliance obligations for our channel relationships, and they are accessible through our partner portal and sustainability webpage.	Provides clear guidance for our go-to-market functions on core policies and procedures, many of which incorporate lessons learned from historical reviews.	Addresses trade restrictions, country-specific guidelines, and export control requirements. This policy promotes compliance with global trade regulations and defines where we conduct business.	Establishes multiple reporting channels for raising concerns and supports protection against retaliation. The policy outlines investigation procedures and escalation protocols, with direct oversight from our board's audit committee, which reviews the policy annually.



Reporting and Investigation

CrowdStrike provides multiple reporting channels, including an anonymous ethics hotline, for employees and stakeholders to raise concerns. Reports undergo a thorough evaluation process, beginning with a preliminary assessment to determine scope and necessary resources.

Matters falling under our Whistleblower Policy are reported to the audit committee, and business unit leaders are responsible for implementing recommended actions. This structured approach consistently handles concerns while maintaining confidentiality and protects against retaliation.

Ethics and Compliance.

Spotlight: Training and Awareness

All CrowdStrike employees are required to complete annual ethics and compliance training. In FY25, we updated this training to enhance its engagement and effectiveness, with CrowdStrike executives delivering key content. The core training covers essential compliance topics, with additional targeted content for go-to-market teams addressing specific risks.

We supplement required training with targeted sessions for specific business units on key topics. FY25 was the first year of our "Ethics and Compliance Week," a voluntary awareness campaign featuring videos, one-pagers, and interactive quizzes covering key compliance topics.

Third-Party Screening

Our comprehensive third-party screening program extends our compliance standards throughout our business ecosystem. We maintain rigorous due diligence procedures for partners and vendors, with ongoing monitoring for adherence to our Business Partner Standards. This approach helps us identify and mitigate potential compliance risks while maintaining strong partner relationships.

Program Effectiveness

This year we saw increased engagement with employees, reflecting CrowdStrikers' growing awareness of our program. In FY26, we plan to further enhance our program by assessing and updating core policies, enhancing our partner compliance network, and developing more data-driven approaches to risk monitoring and program management.

ethics

All CrowdStrike employees are required to complete annual ethics and compliance training.



Stakeholder Engagement.

Building strong, trusted relationships.

In the rapidly evolving world of cybersecurity, our stakeholders are valuable partners in the fight against breaches. Recognizing this, we've built a robust, collaborative framework for engaging with our stockholders, customers, partners, and employees.

Stockholders

We regularly update our stockholders on CrowdStrike's performance and business plans, including our sustainability commitments and initiatives. We are also committed to listening to stockholders and addressing their questions. Through our stockholder engagement program, since our 2024 annual meeting of stockholders, we sought meetings or met with stockholders representing over 40% of our outstanding shares, excluding our affiliates. We also engage with stockholders via quarterly earnings calls, analyst meetings, investor road shows, industry conferences, and company-hosted events.

Customers

Our customers' experiences, challenges, and feedback directly inform our product development and threat intelligence, making us collectively stronger against adversaries. We provide many platforms for customers to engage with us. These include customer and technical advisory boards, biannual surveys and surveys after support interactions, industry security advisory councils, and executive engagement with customers at CrowdStrike conferences and events.

Partners

We offer our channel and distributor, service provider, and technology alliance partners a portal with the sales and marketing tools they need to succeed. We also provide networking and learning opportunities at regional symposiums and global events such as Fal.Con.

Employees

We maintain an open-door management policy at all levels of CrowdStrike. In FY25, we began holding weekly global town halls where all employees can hear from executives and ask questions about our business decisions, strategies, and solutions. We use both informal dialogue with team members and formal feedback like surveys to continually improve our operations and develop new programs. We also use this feedback to strengthen our culture, with an emphasis on creating connections among our global, remote-friendly teams.

JC Herrera | Chief Human Resources Officer



We also provide networking and learning opportunities at regional symposiums and global events such as Fal.Con.

Public Policy.

Engaging on key issues at the intersection of security and technology policy.

CrowdStrike actively engages with policymakers, government agencies, and industry stakeholders to advance cybersecurity policy and protect organizations from cyber threats. We contribute our expertise through congressional testimony, formal responses to proposed regulations, and participation in key industry and government committees. To promote cybersecurity awareness, we share related materials in our [Public Policy Resource Center](#).

Policy Leadership and Engagement

In FY25, CrowdStrike leaders provided expert testimony to the United States Congress on critical issues, including:

- Critical infrastructure protection
- Federal civilian cybersecurity programs
- Healthcare sector cybersecurity
- International cybersecurity threats
- Supply chain security

We actively shape policy development through detailed responses to proposed regulations and frameworks, including:

- Cyber incident reporting requirements
- AI governance
- Data protection and privacy regulations
- Critical infrastructure security
- Financial sector cybersecurity standards

Industry Collaboration

CrowdStrike participates in numerous policy forums and advisory bodies, including:

- The President's National Security Telecommunications Advisory Committee
- The Europol EC3 Advisory Group on Internet Security
- The Information Technology Industry Council
- The Global Cyber Alliance
- Various international cybersecurity and data protection organizations

Through our blog posts, speaking engagements, and policy papers, we share insights on emerging cybersecurity challenges and promote effective policy solutions. Our engagement spans multiple jurisdictions, reflecting the global nature of cyber threats and our commitment to advancing cybersecurity policy worldwide.



Spotlight: Washington Post Live Securing Cyberspace Panel

At a Washington Post Live event hosted by the Washington Post in June 2024, CrowdStrike Vice President of Privacy and Cyber Policy Drew Bagley highlighted the need to address ecosystem-level challenges in our interconnected digital landscape.

Bagley praised initiatives like the Cybersecurity and Infrastructure Security Agency's Secure by Design principles and improved software supply chain security. And he called for coordinated action from federal agencies to develop frameworks for measuring and mitigating concentration risk.

His remarks underscored CrowdStrike's approach to building resilient security solutions that strengthen the entire digital ecosystem rather than creating new vulnerabilities.

Social

Creating a secure future for all.

At CrowdStrike, we embrace the mantra of “One team. One fight.” Our global team is passionate about working together toward our mission to stop breaches, knowing they will be included, supported, and valued along the way. Our mission is rooted in protecting and powering not only our customers but the people and communities they serve. We extend our positive impact further through dedicated social impact initiatives that protect, educate, and uplift our communities.

In this section

25 Our People

- 26 Attracting and Retaining Talent
- 27 Listening and Learning
- 28 Connection and Collaboration
- 29 Benefits and Compensation
- 30 Employee Well-being
- 31 Learning and Development
- 32 Protecting Workers’ Rights

33 Our Communities



Our People.

One team. One fight.

We invest in creating an exceptional employee experience and workplace culture because our people drive our success. The CrowdStrike culture has been built upon our core values since the day we began. We're an action-oriented team that is unified in working toward our mission — a mission that gives us a shared sense of purpose. We hire and develop the best talent based on merit and alignment to our mission, and we provide employees the support and resources they need to do their best work and succeed. This includes a remote-friendly yet connected workplace, comprehensive benefits, well-being programs, and leadership development at all levels. We underscore this with a commitment to protecting workers' rights both among our employees and in our supply chain through policies governing unlawful harassment, discrimination, retaliation, whistleblowing, protected conditions, and health and safety.



CrowdStrike is proud to be Great Place to Work-certified in nine countries: Australia, India, Israel, Japan, Romania, Singapore, Spain, the United Kingdom, and the United States.



One

One team. One fight.

CrowdStrike's Core Values

We are Fanatical About the Customer and Relentlessly Focused on Innovation, and we believe that our Limitless Passion Creates Unlimited Potential for every CrowdStriker.



Attracting and Retaining Talent.

Building a world-class workforce through merit and mission.

We hire and develop people based on their merits and alignment to our mission of stopping breaches. CrowdStrike has been a remote-friendly company since Day One, which enables us to hire the best talent from locations across the world. To attract candidates, we complement our [online job postings](#) with recruiting at industry and university events. Ultimately, our mission, reputation, and results are our greatest strengths in recruiting. The feedback we receive from job candidates tells us they are attracted to CrowdStrike by our balance of growth and stability, our cutting-edge technology, and the opportunity to make a meaningful impact on the world.

We retain talent by rewarding achievement, facilitating connection and collaboration, providing competitive benefits and career development opportunities for all CrowdStrikers, and using employees' input to continuously improve our workplace.

Spotlight: CrowdStrike Global Internship Program

Our global internship program enables us to build a superior talent pipeline and help the next generation grow their careers at CrowdStrike. Through our program, we provide university students and new graduates in 12 countries with a structured, immersive cybersecurity learning experience. Depending on their function, interns work on dedicated projects and rotate through various learning opportunities. All interns have an assigned mentor and networking opportunities. In FY25, we launched our first intern conferences, which brought all of our interns in each region together for 2-3 days of comprehensive professional development workshops, coupled with valuable networking opportunities between interns and leadership.

Employee Onboarding

Our approach to onboarding is designed to provide a "white-glove" experience for every new hire. The process starts with an IT onboarding session on the new hire's first morning to provide a seamless transition to our security-first environment. This is followed by a company orientation and a Core Values workshop. We offer employee onboarding virtually for both remote and office-based employees for a consistent and security-first experience. New hires also attend a remote career development and culture fair to learn about CrowdStrike's training, social impact, and employee experience programs.

We host virtual workshops for new hires at their first 30-, 60-, and 90-day milestones to help them feel connected and supported, and our executive team engages with new hires on a rotating basis to answer questions and offer advice. We also survey new hires throughout their first 90 days to learn what's going well and where we can improve.

65%

Approximately 65% of CrowdStrike's interns join us as entry-level employees.



97%

of employees agree that when you join CrowdStrike, you are made to feel welcome.

Source: 2024 CrowdStrike Trust Index

Listening and Learning.

Using employee insights to elevate our culture.



Just as we use our customers' input to shape our solutions, we use our employees' input to shape our workplace. We've built a comprehensive employee listening program to understand CrowdStrike's priorities and challenges so we can continuously improve their experience. Our goal is to keep employees engaged and excited to grow their careers at CrowdStrike.



Our annual employee engagement survey measures all global employees' satisfaction with aspects of working at CrowdStrike, such as culture, benefits, management, and communication. We also survey employees at important milestones in their journey at CrowdStrike, and we survey employees about their experiences with our events and programs. In FY25, we began using our internally developed AI tools to more frequently survey employee sentiment.



In our FY25 surveys, employees expressed a desire for more frequent interaction with our leaders. We began hosting regular global town hall meetings where CrowdStrike CEO George Kurtz and other executives address timely topics and answer employees' questions. We also used employees' survey responses to shape the features of our Awardco recognition platform that we launched in early FY26.

98%

of CrowdStrike employees say that they are proud to tell others they work here.

Source: 2024 Trust Index



96%

of CrowdStrike employees say it is a great place to work (compared to 57% of employees at a typical U.S.-based company).*

* 2024 Great Place to Work

Connection and Collaboration.

Building community across time zones and teams.

We believe cultivating a connected culture for every employee, no matter where they are in the world, is a key ingredient in building a high-performing company. We encourage community building through in-person and virtual programs. These include our CrowdNeighborhoods program, through which employees plan regular in-person events for their colleagues living nearby. In FY25, we had more than 100 CrowdNeighborhoods chapters across 24 countries. These gatherings complement our in-office CrowdCelebrates events for employees who work in or live near a CrowdStrike office.

We also offer virtual opportunities for CrowdStrikers to connect with their colleagues for support, mentoring, and professional development; to give back to their communities; and to access valuable business insights and innovations.



92%

of employees agree that we celebrate people who try new and better ways of doing things, regardless of outcome.

Source: 2024 CrowdStrike Trust Index

Spotlight: Employee Racing Day

CrowdStrike is heavily involved in racing, led by our CEO George Kurtz’s passion for the sport and the “mission-critical” parallels between racing and cybersecurity. Our [CrowdStrike Racing](#) team competes in SRO Motorsports America, with Kurtz as a driver. In FY25, we hosted two racing days for over 350 CrowdStrikers and their families, where they enjoyed a luncheon at a private suite on the track and garage tours led by CrowdStrike Racing driver Kevin Boehm.



Our nonprofit partner, Operation Motorsport, also gave guests an opportunity to learn more about their mission to use racing to support medically retired veterans in their transition from military to civilian life.



Benefits and Compensation.

Investing in our people.

CrowdStrike offers a competitive total rewards package designed to attract, motivate, and retain top talent. Our goal is to fulfill employees' financial and well-being needs while fostering a sense of ownership and connection.

Key components of our total rewards include:

- Competitive base salaries aligned with market benchmarks
- Performance-driven bonus and commissions programs
- Market-leading equity compensation and Employee Stock Purchase Plan
- Remote-friendly work culture and flexible work arrangements
- Comprehensive health benefits and navigation support
- Retirement plans, including 401(k) plans in the U.S.
- Life and disability income protection insurance
- Employee Assistance Program (EAP)
- Paid parental leave
- Parental and fertility assistance
- Paid time off
- Paid volunteer time off
- Health and wellness programs
- Professional development and mentorship opportunities
- In-office lunch and snacks
- Recognition awards

Flex

Our total rewards include a remote-friendly work culture and flexible work arrangements.



We tailor our total rewards to each country in which we operate, reflecting local market practices, regulatory and compliance requirements, cultural norms and expectations, local labor market trends, currency considerations, and other region-specific factors. For example, in the U.S., we have a “Flex Time Away” policy that empowers employees and managers to collaboratively manage time off while balancing business needs. For countries outside the U.S., we adhere to local labor laws, which often mandate specific vacation time accrual practices.

In FY25, we expanded our benefits to meet the unique needs of our global workforce. In India, we expanded our medical plan to include mental health coverage. We increased time off benefits in Japan and Singapore. In Mexico, we launched new, 100% company-paid insurance offerings. And we rolled out new tax-advantaged retirement plans in Spain, France, and Germany.

We tailor our total rewards to each country in which we operate. Not all total rewards components may be available in every country.

Employee Well-being.

Caring for CrowdStrikers' total well-being.

Our workplace culture is built on pillars of security, well-being, flexibility, appreciation, and enrichment. Our goal is for CrowdStrikers to feel secure and supported, both professionally and personally. Our benefits and programs are designed to support all aspects of our employees' well-being: physical, mental, financial, and community.

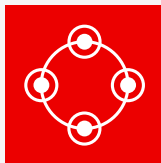
Highlights of our well-being program include:



Mind Health: CrowdStrike's mind health platform powered by Modern Health is designed to support employees at work, at home, and in their relationships. The platform gives CrowdStrikers access to one-on-one sessions with a certified coach, group support sessions, and a library of self-paced courses on topics such as sleep, meditation, and managing stress.



Employee Assistance Program (EAP): Employees can contact a 24/7 crisis phone line for immediate access to a counselor. Our EAP also helps employees find local providers for child care, elder care, financial advisors, legal support, and other life needs.



FalconFit Well-Being Program: FalconFit is designed to empower and support CrowdStrikers in achieving holistic well-being. We provide events, challenges, and education focused on four well-being pillars: physical, mental, financial, and community. Each month, we focus on a different theme.



We offer employees \$30 sponsorships for local wellness activities and competitions.

90%

of employees agree that CrowdStrike is a psychologically and emotionally healthy place to work.

Source: 2024 CrowdStrike Trust Index

In FY25, we organized 50 FalconFit events globally, including in-office massages, fresh juice bars, yoga classes, aromatherapy workshops, charity soccer tournaments, rock climbing, and in-person BBQs. We also installed several treadmill desk stations in our offices. We also continued our FalconFit Lifestyle program, which empowers CrowdStrikers to boost their health through physical activity. Participants receive a CrowdStrike sponsorship of up to \$30 and exclusive FalconFit swag.



Learning and Development.

Accelerating growth at every career stage.

We invest in CrowdStrikers' career growth through comprehensive learning and development programs at all levels, from intern to executive. These programs center around CrowdStrike's core values and the specific behaviors and principles needed to embody them. We also align our performance goals and annual reviews with our values, and our learning programs help employees build the skills to meet these expectations.

We create our programs in-house, so they are tailored to our culture and the specific scenarios our teams face every day. Our dedicated learning and development team works with subject matter experts across CrowdStrike to shape the content, and then the team uses an iterative process to test programs and refine them based on participants' feedback.

Innovative New Offerings

In FY25, we launched a new, enhanced learning management platform that houses both our general leadership development programs and targeted skills trainings. The learning platform also launched for customers and includes our new Falcon Fast Pass, which gives free access to baseline classes.

We are working on integrating AI into our trainings, giving employees the opportunity to practice difficult conversations and receive coaching on their approach. We will roll out this functionality in FY26.

Building Targeted Skills and General Knowledge

In addition to our learning and development programs focused on general leadership and career growth, we offer targeted skills trainings ranging from engineering to sales enablement. All CrowdStrikers have access to GlobeSmart, a platform that improves collaboration with colleagues from different cultures and backgrounds. We also require all employees to take annual trainings on information security, privacy, and our Code of Ethics and Business Conduct.

Key Learning and Development Programs



Falcon Ignite: Leadership skills development program tailored to help individual contributors grow and navigate their unique career paths



Falcon Forward: Managing CrowdStrikers: Self-paced program to strengthen people managers' core competencies as they support the employee life cycle



Falcon Forward: Leading CrowdStrikers: Virtual program that helps people managers cultivate the skills needed to bridge from managing to leading CrowdStrikers



Falcon Forward: Developing CrowdStrikers: In-person program that brings graduates of Managing CrowdStrikers and Leading CrowdStrikers together for an immersive, three-day development experience. This program consistently maintains a participant satisfaction rate of 96% or higher.*

*Source: Qualtrics Survey



87% of employees believe they can access training or development to further themselves professionally.

Source: 2024 CrowdStrike Trust Index

Spotlight: XLR8

Our annual XLR8 challenge gives CrowdStrikers the opportunity to develop a passion project that's incorporated into the company's innovation roadmap, with the potential to be patented and utilized as part of the Falcon platform. Winners of the program are granted generous stock awards. In 2024, nearly 300 employees from 20

countries participated, submitting 151 projects. XLR8 is just one example of how CrowdStrike creates a culture where employees are challenged to think about problems in new and different ways to help our customers stop breaches.

Protecting Workers' Rights.

Promoting fair treatment for all.

CrowdStrike is proud to be an equal opportunity employer. We are committed to fostering a culture of belonging where everyone is valued for who they are and empowered to succeed.

We protect workers' rights through policies governing unlawful harassment, discrimination, retaliation, whistleblowing, protected conditions, and health and safety.

These are summarized in our [Code of Ethics and Business Conduct](#), which we require all employees, officers, board members, and independent contractors to follow.

Zero

Our [Modern Slavery Statement](#) outlines our zero-tolerance approach to modern slavery, human trafficking, and other forced or child labor in our supply chain.



Our Communities.

Protecting, educating, and uplifting our communities.

We are passionate about using our time, talent and expertise to make a positive social impact. Through strategic giving and volunteering, CrowdStrike partners with nonprofits across the world to make our communities stronger and more resilient.

Our Giving Strategy

We focus our corporate philanthropy on areas where our capabilities and perspectives can make the greatest impact. The cybersecurity industry is facing a global shortage of more than 4 million professionals and a critical cyber skills gap, while the threat landscape only continues to grow. We fund scholarships and programs to educate the next generation of cybersecurity professionals. We also donate our software to organizations in need and support nonprofits worldwide — including those focused on veterans support, disaster relief, and education.

CrowdStrike supports these causes through direct contributions, [CrowdStrike Foundation](#) grants, and our donation-matching program for employees. CrowdStrike Foundation grants are managed through our Donor Advised Fund at Charities Aid Foundation America.



CrowdStrike NextGen Scholarship

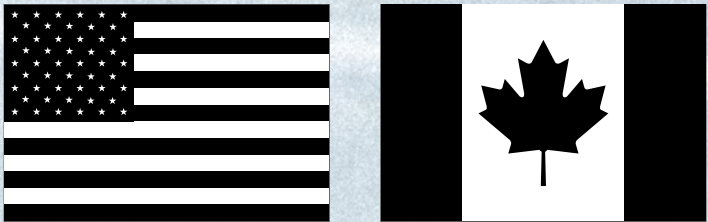
We're committed to helping students build the skills needed for cybersecurity and AI careers. Our NextGen scholarship program provides financial assistance to undergraduate college and graduate students studying cybersecurity and/or AI.



John Amhanesi
NextGen Scholarship
Recipient

60

Since 2017, we've awarded 60
CrowdStrike NextGen Scholarships.



In FY25, we expanded the NextGen scholarship program to junior college students and awarded 18 scholarships to students in the U.S. and Canada.

Our Communities.

Nonprofit Partners

Center for Infrastructure Assurance and Security (CIAS)

Recognizing that students need to build their cybersecurity awareness and knowledge early, this year we launched a partnership with [CIAS](#) to reach middle school and high school students. CrowdStrike is a titanium sponsor of Cyber Threat Defender, a collectible card game that teaches cybersecurity concepts in a fun, engaging way. We worked with CIAS to add a custom card booster pack that features CrowdStrike's cybersecurity solutions and some of the most sophisticated adversaries targeting businesses today.

Our employees support this program by donating card packs to schools and volunteering in classrooms to teach the game. In FY25, we reached over 100,000 students in 28 countries at a critical age for pursuing cybersecurity education, according to CIAS.

CIAS is an organization at The University of Texas at San Antonio that advances the cybersecurity industry through research, training, K-12 education, and collegiate competitions.



Pro Bono Software

CrowdStrike [provides pro bono security software and services](#), including free access to our CrowdStrike Falcon platform, to select nonprofits and nongovernmental organizations (NGOs) across the globe. We recognize that these organizations possess data and intellectual property that make them prime targets for cyberattacks, yet many have limited resources for developing and maintaining effective security programs.



India STEM Foundation

CrowdStrike is a partner of [India STEM Foundation \(ISF\)](#), a nonprofit on a mission to make science, technology, engineering, and mathematics (STEM) education and skill development accessible to all. ISF supports state-of-the-art STEM programs, tinkering labs, infrastructure, and teacher training.

In December 2024, CrowdStrikers in our Pune office hosted 80 students from ISF for a Cyber Threat Defender card game training. Pune employees have volunteered with students from ISF for mentorship events, cybersecurity trainings, and support of the World Robot Olympiad.

Operation Motorsport Foundation

We support [Operation Motorsport](#), a veteran-led nonprofit that aids the recovery and rehabilitation of medically retiring or retired service members through motorsports. Operation Motorsport partners with professional racing teams, including CrowdStrike Racing, to embed program beneficiaries as team members. The skills that make a successful racing team — teamwork, critical thinking, data analytics, and adversary insights — also make a successful cybersecurity team. In FY25, CrowdStrike volunteers held résumé-building and mentoring workshops with beneficiaries and made a gift basket and care kits.

Operation Motorsport Race of Remembrance

In FY25, we continued our tradition of organizing a fundraiser for the [Operation Motorsport Race of Remembrance](#) campaign. At a race in Wales in November 2024, Operation Motorsport held a memorial moment of silence and put the name of a fallen soldier on a race car for every \$22 donated. Former CrowdStrike Chief Security Officer Shawn Henry pledged to match our employees' donations, and together, our team raised \$19,500 for the campaign.



Our Communities.

Local Giving and Volunteering

Through CrowdStrike Cares, we encourage our employees to support local nonprofits and volunteer in the ways that are most meaningful to them.

We have 13 regional volunteer ambassadors around the world, and each year, they support their chosen cybersecurity-related organization. The ambassadors organize company volunteer events, both with nonprofit partners and other local organizations. As a remote-friendly company, we also provide virtual volunteer opportunities, such as online mentorship programs.



We provide every CrowdStriker with eight hours of paid volunteer time off annually and match employees' donations to nonprofits, up to \$100 per person annually.

Global:
Celebrated the winter holidays by giving every CrowdStrike employee a \$50 donation voucher to give to one of five nonprofits.

Denver, Colo.:
Volunteered at the St. Vrain Valley School District Innovation Center to teach students how to play Cyber Threat Defender, an educational card game that teaches cybersecurity concepts.

Sunnyvale, Calif.:
Hosted students from Hofstra University in our Sunnyvale office to share more about our corporate culture and career opportunities in cybersecurity.

Irvine, Calif.:
Mentored students through the BRDG Showcase Challenge, which brings together teams of first-generation college students across multiple disciplines to create a new product focused on sustainability.

San Antonio, Texas:
Sponsored CyberTexas Foundation's 2024 Mayor's Cyber Cup, which drew more than 500 middle and high school students from over 90 schools for competitions and activities. CrowdStrike also sponsored the CyberTexas Summer Camp, where we introduced students to Cyber Threat Defender.

Austin, Texas:
Hosted students from The University of Texas at Austin to learn about cybersecurity roles. CrowdStrike employees volunteered and held Q&A sessions with students at its annual summer camp.



Barcelona, Spain:
Partnered with Asociacion Espanola Contral El Cancer, an organization focused on health education, providing social and psychological care to patients and their families and financing cancer research. CrowdStrikers attended a virtual healthy habits talk to learn more about cancer prevention and volunteered in-person at the annual fundraising cancer walk.

Bucharest, Romania:
Partnered with SOS Satele Copiilor România to educate students about cybersecurity. CrowdStrikers visited an early education classroom to share cybersecurity worksheets and teach about basic cyber safety.

Pune, India:
Hosted 60 students from India STEM Foundation for an event at our Pune office, where CrowdStrikers taught students how to play Cyber Threat Defender.

Singapore:
Hosted over 40 students for a cybersecurity educational event, where students learned about different career paths within cybersecurity and how to protect themselves from cyber threats.

Sydney, Australia:
Partnered with Raise Mentorship, a provider of youth mentoring programs. Students attended an externship day where they visited the CrowdStrike office to learn about careers within cybersecurity and participate in a game based on the CrowdStrike 2024 Global Threat Report.

Local Giving and Volunteering.

Some of our FY25 highlights include:

Environmental

Protecting our planet for today and tomorrow.

As a cloud-native cybersecurity software company with a remote-friendly culture and a small real estate footprint, our direct environmental impact is limited. Nevertheless, we have taken meaningful steps to measure our carbon footprint and energy use, and also evaluate opportunities to reduce our environmental impact where appropriate.

In this section

- 38 Climate Risk and Opportunity
- 39 GHG Emissions and Energy Use
- 42 CrowdStrike Data Centers
- 43 CrowdStrike Offices
- 44 CrowdStrike Operations
- 45 Employee Action
- 46 Sustainability Policies



Climate Risk and Opportunity.

Building foresight and resilience.

We follow a risk management approach for assessing and mitigating risks to CrowdStrike's business, and we understand that climate change is one of these risks. In FY25, we initiated a Climate Risk Scenario Analysis to gain a thorough understanding of the risks that rising temperatures could pose throughout our value chain. The analysis also identified our decarbonization levers — opportunities we can pursue to lower both our risk and our greenhouse gas (GHG) emissions. We engaged a third party to conduct this analysis, with input from our enterprise risk management, facilities, engineering, and finance teams.

See our [TCFD Index](#) for more information on CrowdStrike's management of climate-related risks.

GHG



Through our analysis we also identified our decarbonization levers — opportunities we can pursue to lower both our risk and our greenhouse gas (GHG) emissions.

GHG Emissions and Energy Consumption.

Measuring our impact to drive change.

CrowdStrike is in the business of making data-driven decisions with high accountability to those we serve. To reduce our environmental impact, we have measured our company's GHG emissions footprint and are using this data to inform how we set targets to keep our progress on track.

We submitted our commitment letter in January 2024 to the Science Based Targets initiative (SBTi), expressing our intent to develop near- and long-term company-wide emission reduction targets in line with science-based net-zero standards.

This year, we calculated our FY25 Scope 1 GHG emissions, Scope 2 GHG emissions, and energy consumption for Scope 1 and Scope 2 activities, and had limited assurance procedures performed over the metric quantities by an external third party. See the external [third-party report and management assertion](#), which includes the GHG emissions assessment criteria.

FY25 GHG Emissions

GHG Emissions Metrics	Definition of Metric	Metric Quantity for FY25 (Metric tons CO2e)
Scope 1 GHG emissions	Direct emissions from stationary fuel combustion at leased facilities, mobile fuel combustion by the leased airplane, and refrigerants at leased facilities	3,205
Scope 2 Location-Based GHG emissions	Indirect emissions from purchased electricity and purchased district heat at leased facilities and leased data centers	26,507
Scope 2 Market-Based GHG emissions	Indirect emissions from purchased electricity and purchased district heat at leased facilities and leased data centers	22,277
Reported GHG emissions (Scope 1 and Scope 2 market-based)		25,482

GHG Emissions and Energy Consumption.

FY25 Energy Use

Energy Metric	Definition of Metric	Metric Quantity for FY25 (Mega-watt hours)
Energy consumption for Scope 1 and Scope 2 activities	Energy consumed for Scope 1 and Scope 2 activities at leased facilities and leased data centers	92,078

Energy does not include refrigerants or jet fuel.

Minimizing Our Footprint

To complement our direct efforts to reduce our environmental impact, in FY25, we partnered with Watershed Technology Inc. to identify, purchase, and retire a variety of high-quality energy attribute certificates (EACs).

We previously partnered with ClimeCo and Carbon Fund to identify, purchase, and retire a variety of high-quality, certified carbon offset projects (detailed on [our website](#)) ranging from rainforest conservation to landfill methane removal.

CrowdStrike Data Centers.

Building sustainable digital infrastructure.

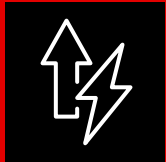
Reducing the environmental impact of our data centers is a key focus area for CrowdStrike because computing is a large component of our energy consumption.



We factor in environmental impact in our data center location selection, preferring locations with sustainable power and a lower carbon footprint. We choose cloud providers and vendors that use renewable energy whenever possible. We continually strive to increase the watts-to-performance ratio of our computing, which increases energy efficiency.



When feasible, we choose servers with lower power demands and adjust the power supply based on demand to minimize energy use. We're also commissioning new customers to data centers with a reduced environmental footprint, and we're optimizing our methodology for impact reporting.



We continually strive to increase the watts-to-performance ratio of our computing, which increases energy efficiency.

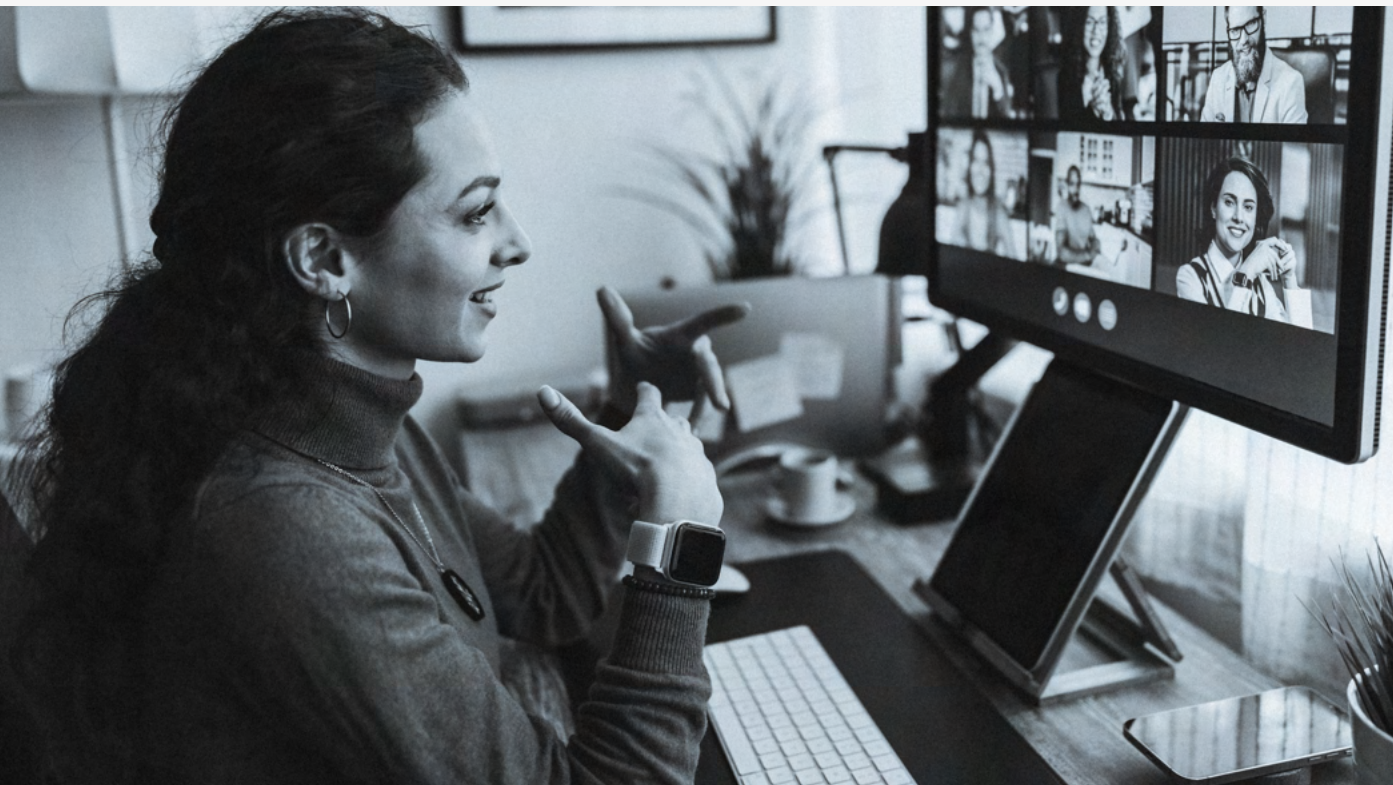


CrowdStrike Offices.

Optimizing our office footprint.

Our remote-friendly culture not only promotes work-life balance but also reduces our need to operate large offices. CrowdStrike has 27 office locations globally. We lease rather than own these facilities, so we reduce our environmental impact by focusing on the factors within our control. That starts with office selection, and our criteria includes choosing new, modern, and resilient spaces that are typically designed to green building standards such as LEED and ENERGY STAR®. We also consider commuting time, looking at the needs of our current and future employee base.

We prioritize green building practices in the construction, build out, and renovation of our interiors. We conserve natural resources through energy and water efficiency, source material reduction, material reuse, and recycling. Because we lease our spaces, each office works with local landlords and vendors on these initiatives. In FY25, we began analyzing these efforts to find opportunities for standardization and scaling best practices across CrowdStrike locations.



60%

of our office buildings are LEED-
or ENERGY STAR®-certified.



CrowdStrike Operations.

Minimizing our operational impact.

Employee Commuting and Travel

CrowdStrike’s remote-friendly culture also reduces our workforce’s overall commuting volume. We encourage virtual meetings, but also balance that with gathering employees in person to maintain strong connections. Large corporate gatherings represent the bulk of our travel, and we are assessing ways to reduce environmental impact. In FY25 we launched a new travel booking system that shows employees the emissions associated with flights so event coordinators and individual employees can make informed decisions. We have also included sustainability-focused language in our Global Hotel RFP, prioritized partnerships with airlines that align with our environmental impact criteria, and encourage use of electric cars for ground transportation.

We also offer a transit benefit that allows employees who commute to receive pre-tax funds to pay for their work-related travel expenses such as transit passes, fare cards and vanpool costs.

Corporate Procurement

In FY25, we began developing a sustainable procurement strategy for CrowdStrike. We assessed our largest spending categories for impact reduction opportunities and considered environmental impact criteria for inclusion in RFPs and purchasing guidelines.



Employee Action.

Creating awareness and grassroots change.

We empower CrowdStrike employees to suggest and implement ideas for reducing our environmental impact. Our Green Team, a global employee interest group with nearly 500 members, drives education and inspires action. The Green Team hosts a speaker series with sustainability activists. It also hosts monthly green challenges to help all CrowdStrike employees build sustainable living habits. Some FY25 highlights included challenges to resist wasteful consumerism and reduce food waste.

Spotlight: Earth Month 2024

To celebrate Earth Day (April 22, 2024), our Green Team planned an entire month of activities to raise CrowdStrikers' awareness of and action on environmental issues. The flagship activity was a Forest Nation Tree Planting Challenge, which encouraged employees to take quizzes on sustainability topics. For each quiz completed, [ForestNation](#) planted 10 trees in CrowdStrike-sponsored forests in Haiti and Tanzania. Together, our team planted 11,800 trees.

Other Earth Month activities included a LinkedIn Learning challenge, a book club discussion, outdoor yoga events and photo challenges, and a virtual terrarium-building event. To celebrate participation in Earth Month, members were asked if they wanted to receive an unbranded recycled tumbler or herb growing kit or make a donation to plant trees through Forest Nation.



500

Our Green Team, a global employee interest group with nearly 500 members, drives education and inspires action.

CrowdStrike Key Sustainability Policies and Resources.

Guiding responsible business conduct.

- Global Privacy Policy
- Information Security Policy & Standards
- [Code of Ethics and Business Conduct](#)
- Anti-bribery and Corruption Policy
- Global Policy Against Unlawful Harassment
- Whistleblower Policy
- [Modern Slavery Statement](#)
- [Business Partner Standards](#)
- Rules of Engagement for Commercial Transactions
- Policy on Lobbying and Political Contributions
- Insider Trading Policy
- [Consolidated EEO-1 Report](#)
- [UK Gender Pay Gap Report](#)

Policies and resources not linked are internal.

Appendix: TCFD Index

California Health and Safety Code Section 38533 Climate-Related Financial Risk Report

As used in this report, references to "CrowdStrike," "we" and "our" refer to CrowdStrike Holdings, Inc. and its subsidiaries.

CrowdStrike is making the following disclosures solely for the purpose of compliance with Section 38533 of the California Health and Safety Code. The inclusion of information in this report should not be construed as a characterization regarding the materiality of that information under any other legal or regulatory regime, including the U.S. federal securities laws. For a discussion of information that is material to CrowdStrike under the U.S. federal securities laws, see our most recently filed Annual Report on Form 10-K and most recently filed Quarterly Report on Form 10-Q. This report is current as of Oct. 27, 2025.

This report contains forward-looking statements that involve risks, uncertainties, and assumptions, including statements regarding CrowdStrike's business strategy, plans, goals and future operational and financial performance; sustainability strategies, initiatives and commitments; climate risk assessment, management and mitigation measures; and long-term outlook. Forward-looking statements are based on current expectations and assumptions as of the date of this report and are subject to known and unknown risks and uncertainties that may cause actual results to differ materially from those expressed or implied by such statements.

These risks include, but are not limited to, risks associated with CrowdStrike's ability to achieve its sustainability goals and to implement related programs successfully; the potential impact of evolving regulatory

frameworks, stakeholder expectations, and disclosure requirements; risks associated with managing rapid growth; CrowdStrike's ability to identify and effectively implement necessary changes to address execution challenges; industry trends; rapidly evolving technological developments; the ability to retain and attract customers and talent; and general market, political, economic, and business conditions, including those related to a deterioration in macroeconomic conditions, inflation, geopolitical uncertainty and conflicts, public health crises, and volatility in the banking and financial services sector.

Additional information regarding these and other risks is included in CrowdStrike's filings with the U.S. Securities and Exchange Commission ("SEC"), including under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" in CrowdStrike's most recently filed Annual Report on Form 10-K, most recently filed Quarterly Report on Form 10-Q, and other SEC filings.

All forward-looking statements in this report are based on information available to CrowdStrike as of the date hereof, and CrowdStrike undertakes no obligation to update any forward-looking statements contained in this report to reflect new information, future events, or otherwise, except as required by applicable law.



Appendix: TCFD Index

Disclosures pursuant to California Health and Safety Code Section 38533(b)(1)(A)(i)

CrowdStrike applied the recommended framework and disclosures contained in the Final Report of Recommendations of the Task Force on Climate-related Financial Disclosures (June 2017) published by the Task Force on Climate-related Financial Disclosures (the “TCFD Reporting Framework”) and has compiled in this report all recommendations and disclosures under the TCFD Reporting Framework that are material to CrowdStrike for the purposes of California Health and Safety Code Section 38533(b)(1)(A)(i).

TCFD Category	TCFD Disclosure	CrowdStrike Response
Governance Disclose the organization's governance around climate-related risks and opportunities.	Describe the board's oversight of climate-related risks and opportunities.	<p>The Board of Directors (Board) oversees CrowdStrike's sustainability and Enterprise Risk Management (ERM) programs, including the assessment and management of climate-related risks and opportunities. The Board is updated as needed on relevant sustainability topics such as regulatory requirements, strategy and goals, priority issues and risks, reporting and assurance.</p> <p>The Board's Audit Committee and Nominating and Corporate Governance Committee both play a role in overseeing sustainability information, including climate-related risks and opportunities.</p> <ul style="list-style-type: none">• Audit Committee: The Audit Committee is responsible for overseeing CrowdStrike's policies and practices relating to risk assessment and risk management. In fulfilling its responsibilities, the Audit Committee reviews and discusses with management, the internal audit function, and the independent auditor, CrowdStrike's major financial risk exposures and steps taken to monitor and control such exposures. The Audit Committee also reviews CrowdStrike's disclosure controls and procedures, discussing with management, and as applicable, the independent auditor, disclosure controls and procedures over environmental and sustainability reporting data and disclosures, as well as any assurance provided by the independent auditor (or other third-parties) with respect to such data and disclosures. These activities are consistent with the Audit Committee's broader responsibility to monitor the integrity of CrowdStrike's financial reporting processes, internal controls, and compliance with legal and regulatory requirements, as outlined in its charter.• Nominating and Corporate Governance Committee: The Nominating and Corporate Governance Committee periodically reviews the Company's sustainability policies, programs, and progress to support the sustainable growth of the business. The Committee also reviews our engagement efforts with stockholders and other key stakeholders related to corporate governance and other applicable sustainability matters.
	Describe management's role in assessing and managing climate-related risks and opportunities.	<p>Multiple business functions are involved in the assessment and management of climate-related risks and opportunities:</p> <ul style="list-style-type: none">• Sustainability: The Sustainability Team leads our sustainability and social impact strategy, reporting and compliance. This includes identifying, assessing and coordinating action on climate-related risks. The Sustainability Team is also responsible for measuring CrowdStrike's greenhouse gas (GHG) emissions and setting goals for GHG reduction. CrowdStrike's Chief Human Resources Officer, who oversees the Sustainability Team, receives periodic updates on initiatives related to reducing our environmental impact and managing climate risk, which are shared at executive meetings.• Enterprise Risk Management (ERM): The ERM Team is responsible for identifying, assessing and prioritizing risks, including climate-related risks, across the enterprise. The ERM Team regularly updates executive leadership and the Board's Audit Committee to support top-level awareness and oversight of CrowdStrike's risk landscape.• Business Resilience: The Business Resilience Team works with ERM to identify risks to CrowdStrike and develop mitigating actions to build resilience.• Finance: The Finance Team provides data inputs for our climate risk analysis, supports calculations around our GHG emissions, and assists with reporting accuracy and oversight.• Legal: The Legal Team supports sustainability regulatory compliance and risk management, and monitors emerging regulatory sustainability trends that may impact the business.• Facilities, Engineering and Procurement: The Facilities, Engineering and Procurement Teams inform risk identification and aid in the development and implementation of climate-related risk and business continuity measures.• Investor Relations: The Investor Relations Team tracks investor inquiries and requirements related to climate and environmental impact.• Sales: The Sales Team tracks customer inquiries and requests related to climate impact.

Appendix: TCFD Index

TCFD Category	TCFD Disclosure	CrowdStrike Response
Risk Management Disclose how the organization identifies, assesses, and manages climate-related risks.	Describe the organization's processes for identifying and assessing climate-related risks.	<p>CrowdStrike undertook our first climate risk assessment in our fiscal year ended January 31, 2025 (FY25) with the support of a third-party consultant. The climate risk assessment included industry benchmarking to identify climate-related risks disclosed by peer companies, customers, partners and suppliers, as well as stakeholder engagement.</p> <p>The climate-related risks identified in this process were subsequently reviewed for relevance to CrowdStrike, and the most relevant climate-related risks were validated with key executive stakeholders and subjected to qualitative scenario analysis.</p> <p>We conducted a scenario analysis across three time horizons, leveraging publicly available climate data and projections, as well as internal data related to CrowdStrike's own operations and supply chain. We assessed risks across the short term (less than one year), medium term (one to five years) and long term (more than five years, up to 2050).</p> <p>We used two climate scenarios from the Intergovernmental Panel on Climate Change (IPCC) 6th Assessment Report (AR6) to perform the analysis.</p> <ul style="list-style-type: none">• The low-emissions scenario (SSP2-1.9) outlines a pathway with low GHG emissions, with estimated warming of 1.4°C by 2100.• The high-emissions scenario (SSP5-8.5) involves very high GHG emissions (high emissions), with estimated warming of 4.4°C by 2100. <p>We considered climate-related physical risks to CrowdStrike's co-located data centers, offices and warehouses; physical risks to our supplier locations; and transition risks related to carbon pricing and technology advancement.</p>
	Describe the organization's processes for managing climate-related risks.	<p>CrowdStrike's risk management strategy includes processes for prioritizing, mitigating, accepting or controlling business risks, including climate-related risks, and involves collaboration across the business.</p> <p>In FY25, our Sustainability Team, working with leaders from our Engineering, Facilities, Procurement, Finance, Business Resilience and ERM Teams, as well as with external consultants, led a scenario analysis to identify, assess and manage CrowdStrike's climate-related risks. The results of the scenario analysis indicated that CrowdStrike's existing processes, including those focused on energy procurement, facility placement, insurance, redundancy, dual sourcing and emergency preparedness, support climate-related risk mitigation.</p>
	Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management.	<p>Our ERM process is designed to identify, assess, manage, monitor and report risks that may impact CrowdStrike. We conducted our climate risk assessment in collaboration with our ERM Team, and the findings were incorporated into our broader ERM results. Additionally, we regularly update our business continuity plans and risk mitigation measures to enhance business resilience and navigate uncertainties such as governmental policy changes, seasonal risk exposure variations and supply chain impacts.</p>

Appendix: TCFD Index

TCFD Category	TCFD Disclosure	CrowdStrike Response
Strategy Disclose the actual and potential impacts of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning where such information is material.	Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term.	A significant natural disaster, such as a fire, a flood, or significant power outage, could have a material adverse impact on our business, results of operations, and financial condition. Natural disasters could affect our personnel, recovery of our assets, data centers, supply chain, manufacturing vendors, or logistics providers’ ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. Climate change could result in an increase in the frequency or severity of natural disasters. If our or our service providers’ information technology systems or manufacturing or logistics abilities are hindered by a natural disaster, shipments could be delayed, resulting in missed financial targets, such as revenue and shipment targets, for a particular quarter.
	Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning.	Although we maintain incident management and disaster response plans, in the event of a major disruption caused by a catastrophic event, such as a natural disaster, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our development activities, and lengthy interruptions in service, and our insurance may not cover such events or may be insufficient to compensate us for the potentially significant losses we may incur. All of the aforementioned risks may be further increased if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, delays in the manufacture, deployment or shipment of our products, or delays in the rendering of our services, our business, financial condition and results of operations would be adversely affected.
	Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario.	CrowdStrike intends to regularly assess its climate-related risks and incorporate this assessment into its overall resilience strategy. We are developing a climate transition plan that focuses on reducing operational emissions, collaborating with partners and providers to reduce value chain emissions, and implementing risk management strategies to strengthen overall business resilience.

Appendix: TCFD Index

TCFD Category	TCFD Disclosure	CrowdStrike Response
Metrics and Targets Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material.	Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process.	CrowdStrike does not consider any metrics used to assess and manage relevant climate-related risks and opportunities material for the purposes of California Health and Safety Code Section 38533(b)(1)(A)(i). As of the date of this report, CrowdStrike has not set any targets to assess and manage relevant climate-related risks and opportunities.
	Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets.	

Disclosures pursuant to California Health and Safety Code Section 38533(b)(1)(A)(ii)

The increasing frequency and severity of natural disasters make redundancy and dual sourcing strategies critical to mitigate the effects of climate change. For this reason, CrowdStrike focuses on data center redundancy, dual sourcing and emergency preparedness for our business and our employees.

