

■ 2025
Corporate
Responsibility
Report

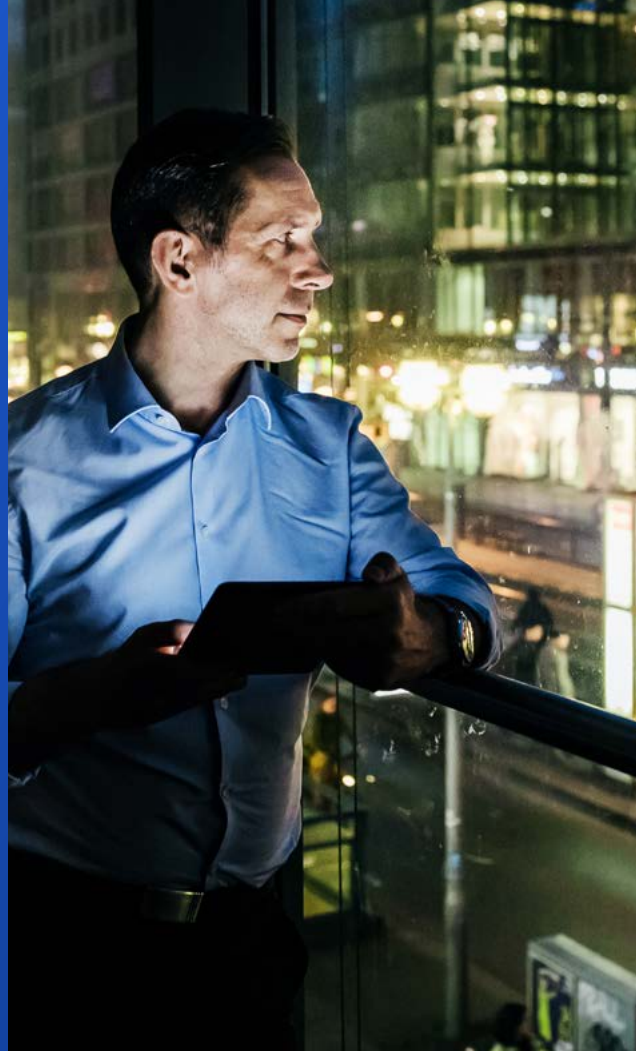


Table of Contents

 **Overview** _____ **2**

 **Governance** _____ **8**

 **Environment** _____ **17**

 **People** _____ **24**

 **Appendix** _____ **33**

About This Report

This report covers Zscaler’s global operations for fiscal year 2025 (August 1, 2024 to July 31, 2025), unless otherwise specified. In line with our commitment to transparency, we publish this report to provide data and context about environmental, social, and governance trends in our business and industry, as well as our operational impacts and progress.

Our approach to corporate responsibility reporting is guided by our company’s legacy of strong business ethics and values. We are pleased to share our journey, highlights from this fiscal year, and focus areas going forward.

For more information, [visit our website](#).

About Zscaler

Zscaler accelerates digital transformation so our customers can be more agile, efficient, resilient, and secure. Our Zero Trust Exchange™ platform implements Zero Trust principles to securely connect users, devices, applications, and workloads, including artificial intelligence, or AI, agents, wherever they are hosted—from any device, anywhere in the world.

Distributed across more than 160 public exchanges and thousands of private exchanges globally, our Secure Access Service Edge (SASE)–based Zero Trust Exchange is the world’s largest inline cloud security platform. Our cloud native, multitenant architecture provides our customers with a comprehensive, flexible, and scalable approach to better secure their operations, optimize user experience, and transform their businesses. With more than 500 billion transactions processed daily, Zscaler provides organizations with the security and confidence to do their best work—whether it’s a hospital caring for patients, a school district educating students, or a company inventing tomorrow’s technology.

Many of the largest enterprises and government agencies in the world rely on our solutions to help accelerate their move to the cloud. We have over 9,400 customers across all

major geographies, spanning every major industry, including financial services, healthcare, consumer goods, insurance, manufacturing, transportation, and more.

We exist to create a world in which the exchange of information is always secure and seamless. Our mission is to anticipate, secure, and simplify the experience of doing business—transforming today and tomorrow. As Zscaler continues to grow and innovate, we will remain focused on delivering solutions that exceed customer expectations and help secure a world of possibility.

Pioneer and Leader in Cloud Security

15+

years of operational experience at scale

PUBLIC COMPANY

since 2018, Nasdaq 100 index component

50M+ CUSTOMERS

50 million+ users protected in 185+ countries

TRUSTED BY

over 45% of Fortune 500

14 consecutive years

as Gartner Magic Quadrant Leader

>75 Net Promoter Score

vs. average NPS of high 30s for SaaS providers

500 BILLION+

daily signals powering AI/ML

700+

issued and pending patents globally



Zscaler Highlights



Our Security Impact

50M+

users
protected

500B+

transactions
processed daily

225M+

cyberthreats
blocked daily



Environmental

100% RENEWABLE

energy for global data centers and offices since 2021

CARBON NEUTRAL

since 2022

NET ZERO GOAL

for operations by 2025 goal achieved



Governance

CORPORATE RESPONSIBILITY

oversight by board committee

SECURITY & PRIVACY

oversight by board committee

CERTIFIED

to over 35 international security and privacy standards



People

95%

of respondents
are aligned
with Zscaler's
mission

92%

know how
their work
contributes
to Zscaler's
success

93%

are proud to
work at Zscaler

Zscaler Zero Trust Exchange™ Platform

The rapid pace of technological innovation is transforming the way organizations operate, compete, and deliver. Data and applications continue to move to the cloud, employees are increasingly mobile, and data is becoming even more valuable with the rise of AI. These developments offer unprecedented possibilities but also introduce new security challenges. Zscaler supports organizations in confidently and effectively overcoming these challenges.

We built the Zero Trust Exchange platform to support companies in accelerating their application, network, and security transformations. Our architecture allows us to extend robust security and policy enforcement to all parts of an organization—across users, cloud applications, devices, and beyond. We help our customers reduce complexity, manage risks, and build more resilient operations.

The Zero Trust Exchange does more than stop threats and enhance security. When enterprises adopt the right tools to defend against cyberthreats and take action based on the valuable data and insights the tools provide, they become more agile, are empowered to push forward, and realize their potential quickly.

Our Approach Enhances Value for Customers

Defends against cyberthreats and protects data: Our solution securely connects users, devices, and applications over any network, replacing firewalls, virtual private networks, and other legacy approaches. We function as a switchboard that controls digital traffic and stops exfiltration of data.

Enables a dynamic workforce: Modernizing the workplace is a business strategy that focuses on people. By providing secure connectivity and data protection regardless of location, Zscaler provides companies with the flexibility to design dynamic workforces that are globally distributed, hybrid, and remote.

Delivers board-level cyber risk insights: Cyber risk has become a greater priority for executives and boards of directors. Zscaler holistically monitors security risks, enabling organizations to develop broader cybersecurity strategies and measure progress. We deliver insights to help customers easily quantify and visualize cyber risk for executive audiences.

Supports environmental efforts: Our cloud-based platform is efficient by design and powered by 100% renewable energy, making it more environmentally sustainable than other options. Our approach also helps customers modernize IT by eliminating hardware and streamlining network infrastructure.

Accelerates secure IT transformation: We partner with customers to replace inefficient security infrastructure with an approach that is more flexible and cost-effective. In doing so, we help them accelerate the adoption of technology while providing a more seamless user experience.

Enhances AI security and governance: Our solutions help organizations safely and securely adopt both public and private AI tools by providing comprehensive visibility, enforcing usage policies, protecting sensitive data, and ensuring compliance through advanced security controls.

How Our Platform Works

The Zero Trust Exchange platform is built using an innovative, cloud-based architecture with inline traffic inspection and advanced threat protection to improve the privacy and security of customers. Our multitenant platform eliminates the need for costly investments in security hardware, supporting business resilience and environmental sustainability.

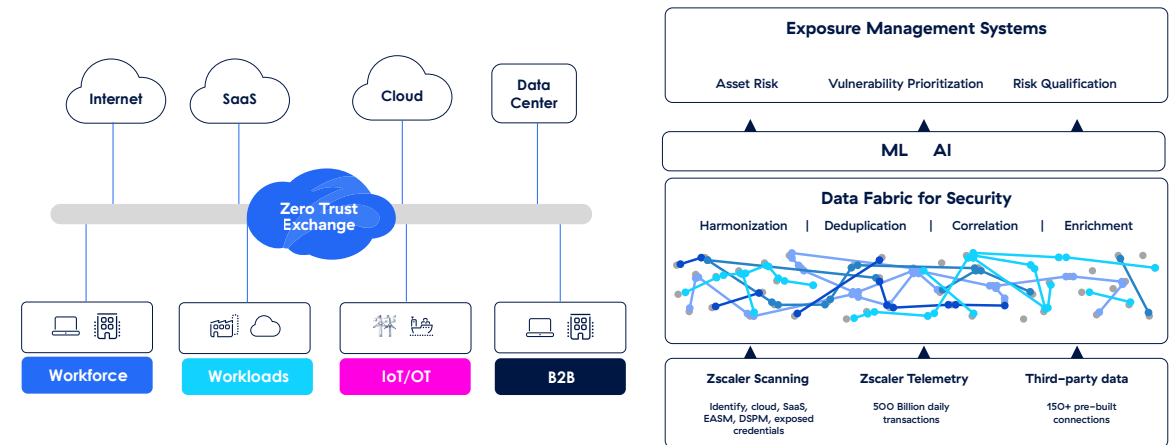
Our Zero Trust architecture intelligently connects thousands of businesses and millions of users to their applications based on credentials and policy. Our approach minimizes the external attack surface of our customers' digital footprint by eliminating exposed public IP addresses. The platform also allows organizations to simplify their IT with Zero Trust connectivity and manage their risks systematically, which can drive broader cybersecurity strategies and remediation projects.

The Zero Trust Exchange platform protects against data loss in two primary ways. First,

our platform enforces policies for sensitive data that are transferred across the web from emails and workloads to devices and other applications. Secondly, our platform prevents risky sharing of company data that is stored in public clouds. It does so without relying on traditional hub-and-spoke network architecture and firewall-centric security technologies, which have become a roadblock to transformation for organizations that want to compete in today's digital world.

Firewalls and virtual private networks, or VPNs, create a perimeter around the corporate network, and everything inside the perimeter is implicitly trusted. This is one of the root causes of ransomware attacks. Zscaler's Zero Trust model operates on the principle that users, workloads, devices, and AI agents are untrusted by default, irrespective of the network they are connected to.

For more information about our platform, [visit our website](#).



Redefining Security with Zero Trust and AI

We believe that Zero Trust combined with AI is rapidly becoming the new foundation for enterprise security architecture. Zscaler is pioneering this convergence of Zero Trust + AI, enabling enterprises to embrace technologies in a manner that is even more secure, scalable, and resilient, while also being increasingly adaptable to the modern world.

Our Approach to Corporate Responsibility

Our ambition is to build an iconic technology company, and we recognize that a thoughtful and intentional approach to corporate responsibility is a key part of this journey. We combine clear priorities, effective governance, and broad implementation to deliver benefits to our customers, employees, investors, and the communities we support.

At Zscaler, corporate responsibility begins with security—the core of our business—and extends through our people-oriented culture, ethical business practices, and environmentally sustainable technology platform. We prioritize efforts that will deliver long-term value and impact for our business and customers, while maintaining a strong commitment to transparently report on our progress.

As the world around us evolves and the expectations of companies change, our corporate values guide our approach to corporate responsibility. The needs of our customers inform our focus areas, as do guidance from relevant and pragmatic reporting frameworks, global regulatory developments, and feedback from investors.

We are committed to delivering an unparalleled platform that secures what our customers do today and unlocks what they dream of doing tomorrow. As our journey continues, we remain focused on the momentum behind us, the world of possibilities ahead, and how we can move forward there together.

Zscaler Corporate Responsibility Focus Areas

Being a trusted partner requires us to understand and address our most important risks, opportunities, and impacts. We continue to refine our priorities based on a changing regulatory environment as well as increasing stakeholder interest in a double materiality approach. In doing so, we look closely at how sustainability issues affect our business and how our activities impact society and the environment.

 Governance	 Environment	 People
Ethical business practices reflect our culture of integrity and responsibility while effectively managing risk.	Efficiency and scale are fundamental to how we operate and reduce our environmental impacts.	Empowering our people and fostering a culture where we function as one team is core to how we serve our customers.
 Business Ethics	 Energy and Climate	 Leadership and Talent Development
 Risk Management and Resilience	 Enabling Green IT	 Employee Engagement
 Information Security and Privacy	 Reducing Waste	 Community Impact
 Secure AI Adoption		



Governance



Zscaler is guided by ethical business practices that reflect a culture of integrity and responsibility. We have developed governance structures and a management approach that help us strike a balance between innovation and accountability.

- Corporate Governance
- Business Conduct and Ethics
- Risk Management
- Information Security and Privacy
- Secure Use of AI

Securing Trust

As a critical partner to more than 9,400 global organizations, we know that robust business practices and strong governance are necessary to secure customer trust and confidence. We strive to operate our business with the highest levels of integrity. That includes our focus on ethical business practices and policies, risk management, and our core mission of ensuring data privacy and information security. The need for strong, effective governance has never been more important than it is today, especially as our industry continues to evolve and truly transformative technologies, such as artificial intelligence (AI), come to market.

Corporate Governance

Zscaler's corporate governance framework provides the controls and structure that allow our business to innovate in today's rapidly changing environment. Our internal teams manage risk and provide updates to management and our Board of Directors (Board) on a range of topics.

For more information on our Board committees, see our [corporate governance documents](#) and [proxy statement](#).

Risk Governance Structure

Board Committees

Audit Committee oversees overall company risk including risks related to privacy and cybersecurity.

Nominating and Corporate Governance Committee oversees our environmental, social, and governance policies, programs, and progress to support our sustainable growth.

Internal Committees

Internal Security Committee manages risks related to privacy and cybersecurity.

Teams

Internal Audit Team continually reviews company procedures and policies to provide reasonable assurance that best practices are followed throughout our organization. The team provides regular updates to the Audit Committee.

Corporate Responsibility Team works cross-functionally across our organization to set strategies and goals, build and embed programs into operations, and track progress.

Business Conduct and Ethics

How we conduct ourselves is just as important as what we do. We are committed to operating our business in an ethical, as well as environmentally and socially responsible, manner. Upholding this commitment underpins our ability to secure the trust of our customers. We are constantly reminded of this responsibility to our customers, who rely on us to protect their businesses, as cyberattacks become increasingly sophisticated, frequent, and damaging.

Our corporate policies define our principles and expectations for employees, suppliers, and third-party partners. The cornerstone of our ethics program, Zscaler's [Code of Conduct](#), describes what we stand for. Our Code of Conduct training, which emphasizes respecting others, acting with integrity, and fostering accountability, is mandatory for Zscaler employees and contractors globally. Other policies and programs that help support our ethical business practices include our [Supplier Code of Conduct](#), as well as our environmental, [privacy](#), anti-corruption, insider trading, political activities, and whistleblower policies.

Every quarter, we require our sales personnel to sign a statement that they have not violated our finance, anti-corruption, and other policies. We train our employees to recognize potential bribery incidents and understand best practices for reporting such incidents. Our legal team regularly reviews Zscaler practices to address potential risks.

Our confidential whistleblower hotline, which is hosted by a third party, is available to all employees, contractors, business partners, suppliers, and others, to report concerns anonymously as allowed by law. We are committed to investigating all reported concerns in a timely manner and take appropriate action when necessary. Zscaler prohibits retaliation against anyone who has reported in good faith a violation of our Code of Conduct, anti-bribery and corruption, or other Zscaler policies.



Risk Management

Trust is the foundation of everything we do, and we earn that trust through a robust approach to identifying, managing, and mitigating risk to our business and operations. We set and update policies, implement effective controls, and conduct internal audits and assessments to manage risks in critical areas of our enterprise. Strategic, financial, business and operational, cybersecurity, privacy, environmental, legal and regulatory compliance, and reputational risks identified through these processes are escalated to management and our Board as appropriate.

Our approach to managing risk in our business includes certifying our solutions to internationally recognized [commercial and government standards](#). These standards help guide our approach to reducing various risks in our operations, so that our customers can adopt our services with confidence.

For more information on our climate risk management approach, see [page 22](#).

Business Resilience and Emergency Preparedness

We consider and regularly review a wide range of potential risks that could affect our business operations.

Our Business Continuity and Disaster Recovery Plan, which is updated annually or as our products and processes change, outlines the steps we take to maintain the global availability of our cloud. Our Cloud Operations Team continuously monitors our platform so that we can respond immediately to issues and maintain resilience in the face of natural disasters or other unplanned emergencies.

With operations in more than 160 data centers globally, we build in fault tolerance wherever possible, providing both intra- and inter-data center redundancy for our production cloud. We also assess the business continuity plans of our data center providers and select partners with the ability to maintain services and connectivity.

We use data and tools to pinpoint issues in the network. This helps us find solutions quickly to meet platform availability and performance targets. We also regularly conduct drills and leverage actual incidents to test our systems and improve the way we manage our platform.

For our global offices and employees, our Facilities Team has developed detailed response plans to guide us through a variety of emergency situations.



Zscaler Resilience™

Our customers depend on the continuous availability of our cloud platform to run their businesses. Our robust failover approaches allow customers to remain operational with minimal customer interaction in the event of minor interruptions. To mitigate catastrophic black swan events that may impact our cloud, we offer and continue to develop business continuity solutions to our customers in a catastrophic event to access critical applications, maintaining security and productivity.

Supply Chain Management

Oversight of our supply chain is essential to Zscaler's operations. Because potential data breaches resulting from supplier vulnerability are a top concern, our vendors undergo robust security risk assessments. Additionally, we conduct extensive due diligence to ensure that our vendors' privacy and security practices are appropriate to their level of data access and the scope of the services they provide. Our vendors must also respect our users' right to access, correct, and delete personal data as outlined in our Privacy Policy. We disclose suppliers that are authorized to process customers' personal data to provide our services and products on our [sub-processors list](#). Such sub-processors are bound by the contractual and legal safeguards set forth in our agreements, including data processing agreements.

We expect all our vendors, suppliers, and other third-party partners to uphold the same high standards of business ethics and integrity that we demand of our own business. We have a rigorous onboarding process in place for new vendors, particularly those who process personal data, when they work with us. This process includes detailed review of their cybersecurity standards and use of AI. Contractors must also complete our data privacy and information security training when initially hired and ongoing

on an annual basis. We conduct security assessments of supplier controls periodically during their engagement. Our reseller partners, which comprise a significant part of our distribution, undergo additional compliance and anti-bribery due diligence reviews.

Our Supplier Code of Conduct outlines our expectations regarding human rights, labor relations, worker health and safety, and environmental protection standards. We periodically conduct reviews of our suppliers to understand if they are at risk of not meeting our social and environmental expectations. If our review determines that a supplier has violated our Supplier Code of Conduct, we will try to work with them to remedy the issue. If the problem persists, we will consider terminating that business relationship.



Information Security and Privacy

Protecting the security and privacy of our customers is a top priority of Zscaler. We believe that privacy is a fundamental human right that is critical to how we build and maintain customer trust. We operate the world's largest security cloud and understand the importance of security by design and privacy by default.

Every day, our platform protects millions of people at thousands of enterprises and government organizations against cyberattacks and data breaches. We invest in the people, processes, and technologies that support the security, privacy, and resilience needed to deliver a world-class platform.

Cybersecurity Governance

The Zscaler platform leverages guidance from leading industry frameworks to effectively manage and mitigate cybersecurity risks. Our rigorous risk management processes cover data privacy, product security, and information security to ensure the highest levels of confidentiality, integrity, and availability for our customers. We continuously evaluate the performance, and strengthen the security, of our products to anticipate the evolving threat landscape. We engage with customers, external experts,

and industry groups with diverse perspectives so that we can continue to deliver innovative solutions.

The Audit Committee of the Board oversees cybersecurity risk, with input from our internal security committee. The internal security committee identifies and prioritizes protective measures across our enterprise and products, driving improvements to our security approach as threats evolve. The committee is led by our chief security officer, who regularly reports to our management team and CEO, and includes representatives from our security team, information technology, information security, incident response, engineering, enterprise risk, product management, cloud operations, legal, and compliance teams.

These key functional leaders share critical information and use data-driven strategies to manage cyber risks. The internal security committee meets at least monthly, updates the Audit Committee quarterly, and apprises the full Board as needed.



Cybersecurity Is a Core Business Issue

Cybersecurity is a core business issue for all companies in the digital age as investors, regulators, and other stakeholders increase their demands for company disclosure on cybersecurity incidents and risk management.

We are helping our customers' executive teams and boards of directors better understand the risk posture of their organization through a risk quantification framework and dashboard called Risk360. This offering provides unparalleled visibility, with up-to-date security status and corrective actions they can take in a timely fashion.

Global Commercial Certifications



Global Government Certifications



For a full list of our security and privacy certifications, visit our [Compliance webpage](#).

Cybersecurity Approach

We continuously review our cybersecurity policies, standards, and procedures to account for changes in the threat landscape, as well as in response to legal and regulatory developments. Our cybersecurity efforts also include mandatory training for all employees and contractors on our security and privacy policies.

Our compliance team works to ensure that Zscaler products are aligned with, and certified against, the rigorous requirements of internationally recognized commercial and government [standards](#).

We implement security checks and reviews throughout our development lifecycle, and our internal security teams and external cybersecurity auditors continuously evaluate our products. Our cloud platform is monitored in real time, and we provide publicly available insights into the performance and health of our services. Our [Trust Portal](#) displays updated statuses and advisories. In addition to improving Zscaler's products, the team shares its research with the wider industry to promote a safer internet.

Our in-house global threat research team, [Zscaler ThreatLabz](#), has a mission to protect our customers from advanced cyberthreats. Armed with insights from over 500 billion daily signals on our platform, more than 150 security experts collectively operate 24/7/365 to identify and prevent emerging threats. They do so using malware reverse engineering, behavior analytics, data science, and AI.

Our incident response plan includes processes and procedures for assessing potential internal and external threats, activation and notification, and crisis management. The plan also includes assigned roles and responsibilities and escalation procedures in the case of potential security incidents. Our approach includes procedures to inform management, the Audit Committee, and the Board of cybersecurity threats and incidents. Post-incident analysis is designed to safeguard and strengthen the confidentiality, availability, and integrity of our platform and assets going forward.

Privacy Approach

Our detailed policies—covering employees, customers, and third parties—govern our data management and use practices. We periodically update our policies in light of new regulatory requirements, technology advancements and best practices, and customer needs. We are transparent with our customers about how we handle their data.

To help our customers comply with local privacy laws, we implement technical and organizational measures for customer data that pass through our Zero Trust Exchange platform. By default, Zscaler products set privacy settings to maximum confidentiality.

Zscaler conducts privacy impact assessments prior to the release of our products to ensure that new products or updates to existing features comply with applicable data protection laws and regulations.

When offered as a commercial option, customers can choose to have transaction logs stored exclusively in the United States or the European Union/Switzerland, regardless of where their users happen to be accessing Zscaler products. Additionally, we provide our customers with the ability to configure which of our global data center

locations process their data, according to their compliance needs. The transaction logs are retained by Zscaler for the applicable data retention period during the term of subscription.

Our full-time, certified privacy professionals and our global security compliance team are responsible for day-to-day management of our privacy program, ensuring that we meet our obligations and requirements under various privacy and security certifications. To protect both Zscaler and customer assets, we require all our employees to complete our extensive data privacy and information security training when they are hired and annually thereafter.

We also publish a [Transparency Report](#) that discloses the number of requests we receive from government agencies, regulatory bodies, and law enforcement regarding Zscaler customers' use of Zscaler products. In 2025, we received 107 such requests and did not disclose our users' personal data. If Zscaler is legally required to disclose any personal data of a customer's user, we will promptly notify the customer before making any such disclosure unless prohibited from doing so by law.

The Zscaler corporate website is subject to our [Privacy Policy](#), which respects our users' right to access, correct, and delete personal data. We collect personal data only for specific, explicit, and legitimate business purposes, and we store that data only for the period necessary to achieve the purpose of the storage, or as permitted by law. The policy also contains language to reflect our compliance with the EU-US Data Privacy Framework, U.K. Extension of the Data Privacy Framework, and Swiss-US Data Privacy Framework.

For more information about our data privacy practices, visit our [Data Privacy and Protection webpage](#).

Inspection of Customer Data

Our customers trust us to process their data with care. As a data processor, we only process personal data on behalf of our customers—the data controllers—when they provide us with documented authorization. We contractually uphold this responsibility through our Data Processing Agreement.

Without prior authorization, customers' network and internet transaction content is not stored or written to disk; inspections take place only in memory. Once inspection is complete and no threat is identified, data flow continues unimpeded, with no record of the source data preserved beyond tokenized audit logs of the transaction.

Secure Use of AI

AI is helping shape the future of work, communication, information, and many other areas of our lives. We believe that Zscaler has a critical role to play in enabling the responsible use of this technology for our customers. We also recognize that emerging technologies like AI must be continually scrutinized to make sure we have a clear understanding of both its strengths and any potential shortcomings.

Our Responsible Use of AI

Our solutions incorporate AI and machine learning to develop increasingly sophisticated defenses against ransomware and other attacks. Threat actors are also advancing their use of AI, but the scale and quality of our data make us uniquely positioned to counter their activities. Zscaler processes more than 500 billion logged transactions each day from over 50 million users globally, which enables us to identify patterns and develop countermeasures.

Along with the transformative opportunities AI presents, developing and deploying it require careful attention to make sure that the technology is used safely and responsibly throughout the AI lifecycle. Our AI development efforts, as well as employee use of approved AI tools, must comply with Zscaler policies. These policies establish frameworks and guidelines to ensure that AI is deployed securely, balances

ethical considerations, and meets emerging regulations. A consistently applied framework also protects the interests of our company, employees, customers, and partners. We evaluate new and recurring uses of AI to ensure we adopt this technology responsibly and effectively.

Vendors that may use AI are subject to our AI due diligence process, which evaluates:

- The categories and sensitivity of the data process; compliance with applicable data protection and privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA);
- Permissible use of our data in learning models including restrictions on using our data to train generalized models;
- Data residency, retention, and storage controls; and
- Environment segmentation and tenancy isolation to prevent cross-customer data leakage—while also identifying and mitigating ethical risks.

Supporting Customer Adoption of AI

Companies in every industry are embracing generative AI solutions for their potential to unlock insights, improve employee productivity, and solve complex problems. At the

same time, adopting this technology increases exposure to security risks, resulting in some companies banning the use of AI completely.

We believe that AI is simply too powerful for our customers to ignore, but it requires a carefully considered approach. Through the Zscaler Zero Trust Exchange, we enable our customers to safely adopt and realize the benefits of AI in ways that are best for their businesses. That includes helping our customers create and enforce policies for addressing generative AI applications that their employees access and use. Our platform helps customers prevent AI-related data leakage by setting policies on data and model use, inspecting prompts and outputs in real time, and redacting or blocking sensitive content.

As AI's capabilities expand, we will continue to assess its potential benefits for both Zscaler and our customers, while continuously evaluating the evolving risk and threat landscape and the need for additional oversight, governance, and controls.

Leveraging AI Without Sacrificing Customer Privacy

As Zscaler works to safely unlock the value of AI, we want to make sure that our efforts don't come at the expense of customer privacy. We do not use any proprietary customer information or personal data to train our AI models. Instead, Zscaler leverages the aggregate knowledge of signals across our platform to strengthen detection and modeling.

Every customer's data tenancy is self-contained and under their control. Logs, transactions, and telemetry generated by their use of our platform are used to improve outcomes for their organization alone. Customers benefit directly from their own signals, whether it's for risk modeling, AI copilots, or policy enforcement, without having to trade away autonomy, privacy, or security.

For more information on how we secure the use of AI, [please read here.](#)





Environment



Zscaler's commitment to environmental stewardship is reflected in how we operate and is integral to the value we provide to our customers.

- Delivering Environmental Benefits
- Cybersecurity Life Cycle Assessment
- Managing Environmental Impacts and Waste
- Our Carbon Footprint
- Climate Risk and Opportunity

Embedding Environmental Efficiency

The cloud native Zscaler Zero Trust Exchange™ platform enables significant hardware reduction and energy efficiency improvements over legacy on-premises solutions. Based on our product life cycle assessment (LCA), our solutions use up to 93% less energy and result in 15 times lower emissions. Our architecture, optimized processing, and use of renewable energy all contribute to a less emissions-intensive solution that helps enable our customers to achieve their own environmental goals.

We use a holistic approach to manage our climate risks and to deliver a more resilient cybersecurity solution. In addition to addressing climate impacts, we are taking a mindful approach to managing waste, including by repairing, reusing, and recycling hardware.

Delivering Environmental Benefits

When customers entrust us with securing their business, they can confidently accelerate their digital transformation, while realizing key environmental benefits:



Minimize IT waste: Our cloud-based approach reduces our customers' need to purchase, manage, and replace hardware. We also take a responsible approach to minimizing the waste that comes from our own hardware use.



Reduce carbon footprint: We help customers lower the greenhouse gas (GHG) emissions associated with their security program as our Zero Trust Exchange platform is powered by 100% renewable energy.

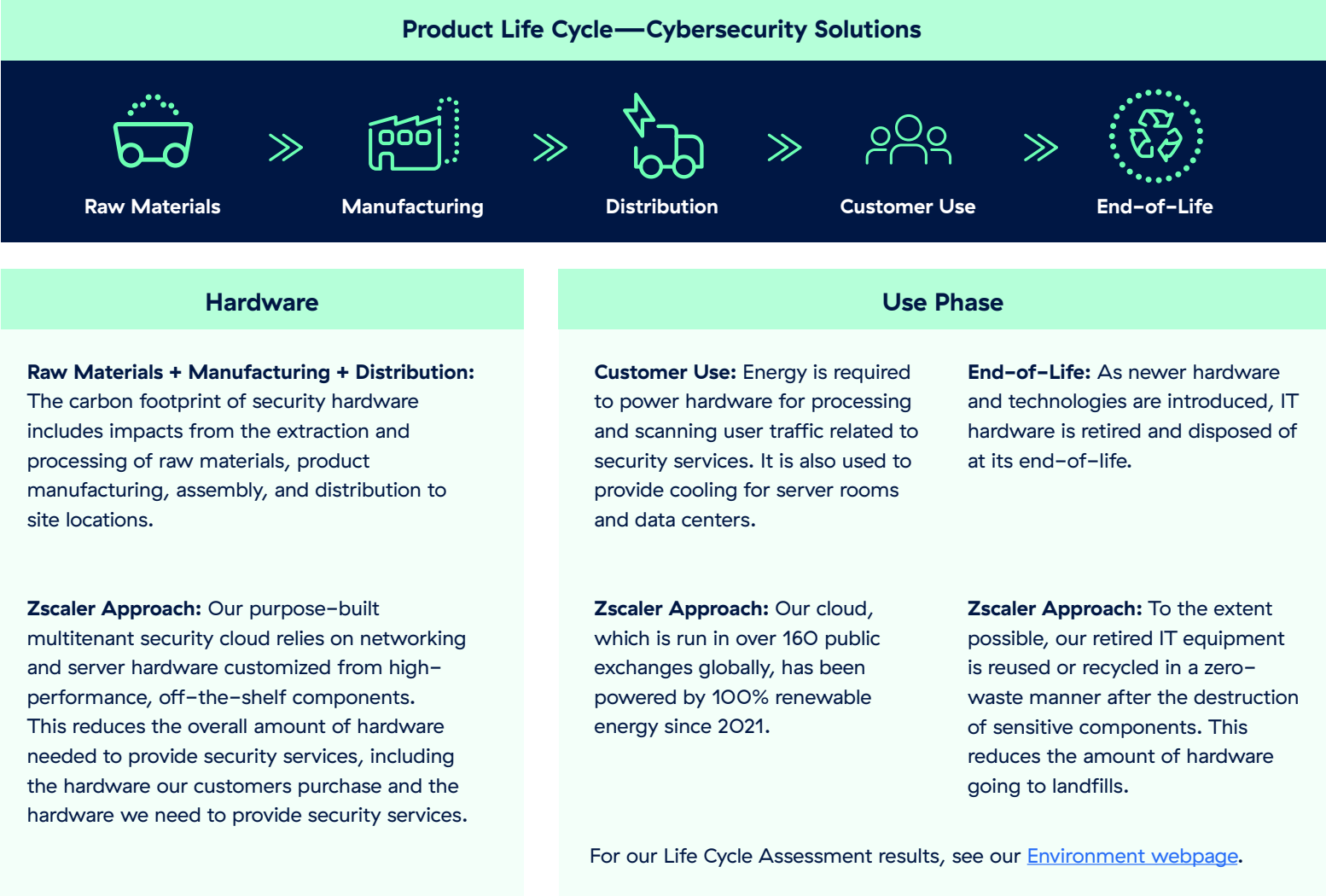


Lower energy consumption: We deliver better security using less energy per comparable unit of functionality with a purpose-built multitenant cloud security solution.



Support remote access for every user: By supporting employees and third-party partners anywhere, on any device, we help customers reduce everyday emissions from employee commutes and business travel.

Reducing Environmental Impact Across the Cybersecurity Life Cycle: Zscaler vs. Legacy Solutions



Up to **93%**
reduction in
energy usage*

*When comparing energy usage required for providing 1 year of cybersecurity for an organization.

Our Approach to Managing Environmental Impacts

We take a pragmatic, results- and data-driven approach to environmental management, to identify and enable us to focus on where we can effectively address impacts, risks, and opportunities. Our Environmental Policy outlines our objectives related to ensuring compliance, managing environmental risks and impacts, committing to renewable energy and climate action, and engaging key supply chain partners.

Through conducting a life cycle assessment we have determined that a significant impact within our direct operations is the electricity used to power our cloud in more than 160 data centers around the globe. As a result, engaging with our data center providers on energy efficiency and renewable energy use is a priority.

Given the progress we have made in using renewable energy to reduce our carbon footprint, we have expanded our focus to other emissions sources.

As with other software companies, this includes Scope 3 emissions in categories such as procurement and business travel—where our influence may be limited or broader, more collective reduction efforts are needed. Further analysis in FY2024 showed that among Scope 3 categories, the procurement of computer hardware is a large source of our indirect emissions. We will continue to optimize our use of hardware and deploy efficient infrastructure while deliberately managing waste.

We continue to assess and manage other potential environmental impacts. In 2025, we assessed the potential biodiversity impacts of key stages in our operations. This assessment determined no significant biodiversity impacts in our locations; however, we will continue to regularly evaluate any changes that may inform our approach. We also strive to manage waste-related impacts by continuing to optimize our use of hardware and deploy efficient infrastructure.

Energy-Efficient Platform Architecture by Design

The Zscaler Zero Trust Exchange platform is built on a cloud native architecture engineered to be more efficient than legacy solutions:

- Using optimized hardware to build a true multitenant solution from the ground up enables us to better match capacity with users. This improves performance while reducing idling hardware and wasted resources.
- Deploying our own service edge reduces computational overhead and allows for faster processing as opposed to virtualization.
- Innovations such as our Single-Scan Multiple Action engine drastically reduce resources used compared to the service chaining approach of legacy platforms, which require data to be passed along multiple point product appliances for the same level of protection.
- Optimizations to our platform help achieve better traffic density per unit of hardware, improve performance, and reduce energy needs. New hardware and code enhancements, such as using advanced threading technology, increase concurrent processing and further improve our overall efficiency.

Managing the Environmental Impact of AI Technologies

AI has tremendous potential to help our customers drive their business forward and enables us to deliver better protection. We are taking a thoughtful approach to embedding AI into our processes and customer solutions. In addition to focusing on security and the responsible use of AI, we also recognize that AI technologies are driving increased resource demands and emissions. As with all our products, we are optimizing efficiency and focusing on where we can effectively address impacts. Our use of AI, including model training and employee usage, is either powered by 100% renewable or carbon-free energy, or matched with carbon offsets.

Reducing the Carbon Impact of Cloud Operations

To deliver for our customers, we strategically select data centers that have the highest levels of security, are located close to users, and are operationally reliable. We also take into account the carbon impact of our cloud operations.

As we continue to expand our cloud, managing energy use with our data center providers is increasingly important. Our data center selection and renewal processes integrate sustainability criteria. Where possible, we prioritize data center providers that use renewable energy, have their own climate goals, and achieve efficiency through other practices, such as motion-activated LED lights, automated controls, hot and cold aisle containment, and liquid cooling.

We engage with our data center providers through an annual environmental survey to further understand and track their practices and performance. In 2025, we received responses representing more than 98% of our data center capacity. We use this annual survey, as well as regular business reviews, to more deeply engage with our data center providers on ways to reduce emissions and other environmental impacts and hold them accountable during renewal periods.

We are committed to continuing to power our cloud with 100% renewable energy even as our business grows. Many of our data center providers use renewable energy to power some or all of their facilities. To account for any

Zscaler energy consumption from non-renewable sources, we purchase high-quality renewable energy credits from country-specific wind and solar projects. As an edge service provider, our solution spans more than 160 public exchanges globally—applying renewable energy credits is the practical approach we have taken given the geographic spread of our energy use.

Managing Waste

Our cloud-based services provide customers with the benefit of reducing server waste and costly hardware upgrades associated with cybersecurity. We take a responsible approach to managing our two primary waste streams: hardware and office waste.

We deploy server hardware with efficiency, performance, and longevity in mind, which also optimizes for environmental sustainability. We have extended the lifespan of our hardware from four years to five years—which means better use of resources and less waste, while taking into account the tradeoff of using more efficient new hardware. Whenever possible, we service or repair hardware, and at server end-of-life, the vast majority is reused or recycled. We partner with a third party that clears, sanitizes, and physically shreds sensitive components to destroy data. Our vendor then repurposes working parts and recycles the remaining materials.

As our global employee count grows, we use flexible working spaces in many regions to optimize office space utilization. This, combined with our hybrid work approach, has helped us reduce office waste. In addition, we responsibly manage e-waste for the IT hardware that our employees use and diverted over 715 pounds from landfills during the past year.

Zero Trust SD-WAN for Branches

Our core Zero Trust Everywhere products help to reduce the hardware needed at client sites. Our Zero Trust SD-WAN solution is a simple on-premise appliance that securely connects branches, campuses, and factories. We are monitoring the environmental impacts of this hardware, and we plan to conduct a Lifecycle Assessment (LCA) to assess its emissions profile in 2026. In the meantime, we are purchasing renewable energy credits to offset the emissions resulting from customer usage.

Our Carbon Footprint

Mitigating Carbon Impacts

We are committed to understanding our carbon impacts as we operate our business to support our evolving customer needs. Though our solution already delivers a range of environmental benefits to our customers, we continue to look for ways to reduce our carbon impacts. We calculate and monitor our emissions across all relevant categories in alignment with the Greenhouse Gas Protocol. We continue to work with our suppliers to gather data that accurately reflects our energy consumption and emissions.

We are pleased to have met our 2025 goal to reach net zero for our Scope 1 and 2 emissions covering our operations. Our progress was supported through operational efficiency efforts and purchasing renewable energy and offsets.

To align our approach with global efforts and better support our customers’ sustainability initiatives, we have committed to develop a science-based target, in line with the global goal to limit global warming to well below 1.5°C above pre-industrial levels, and we have engaged with the Science Based Targets initiative on target validation.

We will continue to share our progress so that our customers have confidence that they are working with a partner aligned with their climate goals.

GHG Emissions by Scope

Greenhouse Gas Emissions (MTCO ₂ e)			
Scope	CY 2022	CY 2023	CY 2024
Scope 1 – Total	277*	340*	439*
Scope 2 – Location-based <i>Electricity used at data centers and offices</i>	22,877	22,439	28,198
Scope 2 – Market-based <i>After application of energy attribute certificates</i>	0	0	0
Scope 3 – Total	36,738*	46,304*	54,668*
Total Emissions – Location-based	59,892*	69,083*	83,305*
Intensity: MTCO ₂ e / revenue (\$m)**	17.2	12.0	11.8

*Does not include the application of voluntarily purchased carbon offsets that cover 100% of the Scope 1 and 3 emissions categories.
**Calculated using Scope 1 and 2 (location-based) emissions.

Year-Over-Year Emissions Changes

Our absolute emissions increased in calendar year 2024, due to the need for additional energy to support business growth. However, our emissions intensity improved, illustrating that as our business continues to expand, we are operating more efficiently.

Our Scope 2 emissions increased as office space and data center usage increased with our growing business. We also continued to see improvements in data quality from our data center providers. Scope 3 emissions also increased, reflecting overall business growth.

For more details, please see our GHG [verification statement](#).

Climate Risk and Opportunity

We take a comprehensive approach to assessing and managing climate risk across the key areas of our business, which helps us understand where our operations may need to adapt. This includes a risk management process in which a cross-functional team identifies, assesses, and responds to climate-related risks and opportunities.

We conduct this analysis annually and whenever there is a substantial change to our business. We also work with our internal business partners on an ongoing basis to factor climate risk and impacts into their planning. We undertake a similar process for identifying, assessing, and addressing climate-related opportunities.

Climate Risk Governance

Our Nominating and Corporate Governance Committee oversees our corporate sustainability program, including the review of climate risks, opportunities, and progress. If material climate risks are identified, our Audit Committee evaluates them for potential financial risk exposures and outlines the steps our management team will take to monitor and control them.

Climate Risk Management Approach

1. Identify

Our climate risk process starts with identifying and mapping the risk types across our value chain, including physical and transitional risks to our data centers, suppliers, offices, and workforce.

2. Assess

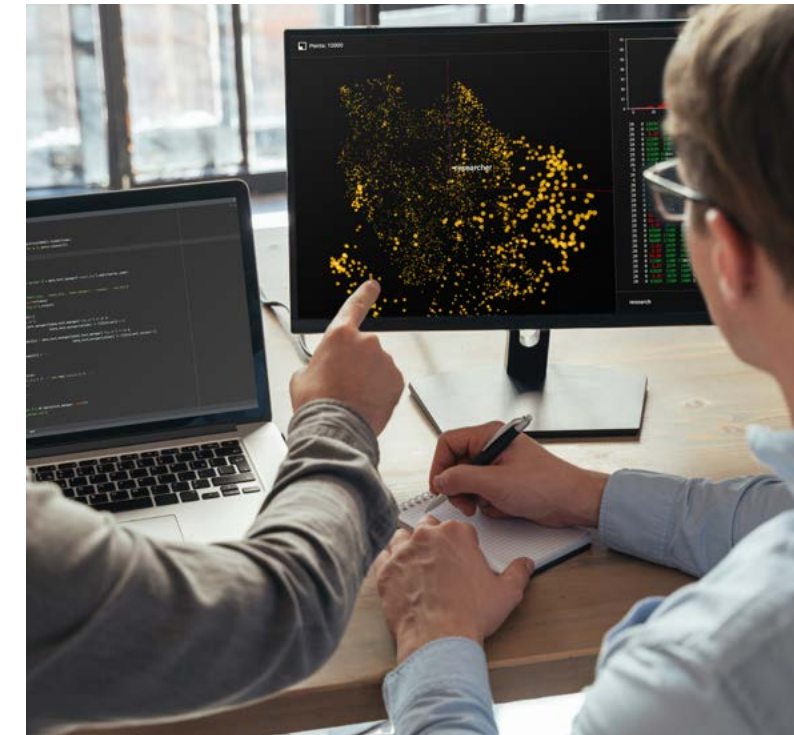
Identified risk areas are assessed across value chain stages, time horizons, geographies, and financial impacts, using quantitative and qualitative methods to understand the impact to our business. We also consider water stress, flood, and heat index data for physical locations and track regulatory developments impacting our sector.

3. Address

If climate-related risks without sufficient mitigations are identified, the findings are shared with subject matter experts and leaders for review and response. Input from these experts helps validate risks and determine appropriate action plans.

4. Report

Results of our annual climate risk assessments are reported to the Nominating and Corporate Governance Committee, which oversees our corporate responsibility program and monitors progress. If any material financial exposures are identified, the Audit Committee reviews them and works closely with management on monitoring and mitigation strategies.



Climate Risk and Opportunity Assessment Results

Our annual risk assessment of more than 85 potential climate-related risks considers any changes in our operations and business activities relative to the prior year. In our most recent analysis, we did not identify any climate-related risks or opportunities with the potential to have a substantive financial or strategic impact on our business. This is partly due to our efforts to design our product architecture and business operations in ways that are resilient to climate risks.

As climate-related extreme weather events occur with increasing frequency in broader geographic areas, we are committed to assessing physical risks and updating our approach regularly. We will also assess the changing drivers of transitional risks and continue to monitor changes to our business. We will strengthen our operations as relevant.

Climate Resilience and Adaptation by Design

The results of our most recent climate risk assessment continued to reveal that our cloud is resilient against the physical impacts of climate change, including outages caused by storms, heat, or other climate-related disruptions.

Zscaler's highly redundant, distributed global platform—built and maintained so that our cloud is reliable, available, secure, and serviceable—means that climate resilience is inherent in how we operate. We engineer our solution so that if any region or data center experiences an outage, we have the capacity and dynamic failover capabilities to quickly reroute user traffic to unaffected geographies, ensuring uninterrupted platform availability. Additionally, we use data centers with robust continuity plans, and our largest sites are located in areas with relatively low physical climate risk.

We aim to reduce our customers' exposure to climate risk through our product solutions. As climate change continues to create chronic events, such as prolonged heat waves, storms, and fires, this may increase the need for more businesses to move to the cloud, adopt hybrid work environments, and plan for business continuity.

We are hopeful these organizations will turn to Zscaler to accelerate their digital transformation, so that together we can build a more climate-resilient world.

We have also updated our practices to help keep our growing number of global employees safe and informed in the face of increasing instances of extreme weather. We utilize a sophisticated communications tool that provides employees with advanced warning of localized weather events or other alerts to enable them to stay connected during active emergencies.

While our assessments currently show minimal exposure to substantive climate-related financial risks, Zscaler remains vigilant. We are committed to re-assessing risk in response to an evolving climate landscape, adapting and strengthening our mitigation strategies, and maintaining robust operational resilience for both Zscaler and its customers.

More information is available in our [TCFD Index](#) and our [CDP response](#).



Empowering our people is at the core of how we deliver. By giving our people the right tools and development opportunities to grow with Zscaler, we facilitate collaboration, innovation, and high performance, all of which drive value for our customers and help build a more secure future.

- Zscaler Culture and Values
- Talent Attraction and Retention
- Compensation and Benefits
- Employee Development
- Employee Engagement
- Community Impact

Enabling Possibility for People

Zscaler products help customers foster innovation, workplace flexibility, and strong employee performance by enabling safety, security, and resilience in an increasingly complex digital and AI-driven world.

We start by bringing in exceptional talent and nurturing a positive culture where employees can thrive, building upon our strong values and a shared mission. We are intentional about creating an employee experience where everyone at Zscaler can feel a sense of pride, purpose, and belonging. We continually work to support our employees in their professional and personal lives so that they are empowered to do their best work.

Zscaler Culture and Values

We're proud of our culture of teamwork and innovation, which prioritizes providing value to our customers. We strive to create a work environment where employees are encouraged to test new ideas, push boundaries, and solve big challenges. Our people are collaborative, curious, hardworking, and dedicated to assisting our customers and one another.

We are driven to transform the cybersecurity landscape and believe we are uniquely positioned to succeed with a passionate team focused on achieving our ambitious company objectives. Zscaler's culture is grounded in our shared mission to anticipate, secure, and simplify the experience of doing business. Our TOPIC [values](#) help us deliver on this mission by guiding how we work to support each other and our customers.

Our Values



Teamwork



Ownership



Passion



Innovation



Customer Obsession

We recently refreshed our values to reflect our culture of ownership. For more information on our Values, [visit our website](#).

Talent Attraction and Retention

Zscaler is a destination for top talent looking to make a difference at a mission-driven company, revolutionizing security around the world. Zscaler works to attract and retain high-performing individuals by recruiting from a broad talent pool and then providing competitive compensation and benefits, including support for our employees' overall well-being.

Recruiting Quality Talent

Our talent attraction strategy is focused on building the next generation of cybersecurity and go-to-market leaders. We have continued to strengthen our leadership team by bringing in key hires to support the company's evolution.

Attracting and hiring the best talent will help us strengthen our platform, launch new products to delight our customers, and execute our ambitious growth plans. Here are a few of our efforts aimed at ensuring a high-quality talent pipeline:

- Employee referral program
- Internship program that provides students and recent graduates with meaningful work experience
- Dedicated Executive Recruiting team focused on leadership roles

- Proactive branding and event sponsorship strategy to foster careers at Zscaler and open doors for those interested in exploring cybersecurity
- Structured interview process designed to broaden our qualified talent pools

We believe that attracting and supporting a workforce that is representative of the customers we serve helps us better anticipate their needs and solve their challenges. Zscaler has invested in training on how to create fairness in hiring, and we continue to assess ways of improving the candidate experience. In addition, we take a global approach to attracting and hiring the best talent rather than just focusing on our established hubs.



Providing Opportunities for Service Members and Veterans

Zscaler values the skills and experiences of military service members and veterans, and we are committed to fostering a work environment where they can build meaningful careers and make a lasting impact. For example, we participate in the U.S. Department of Defense/War SkillBridge program, which provides U.S. service members with opportunities to explore a transition into civilian careers.

In 2025, Zscaler also rolled out expanded military leave benefits. Among them, we increased our short-term military leave policy for U.S. employees from 10 to 30 workdays with full pay and benefits. We introduced a new long-term military leave benefit as well, which provides top-up pay and health coverage for leaves greater than 30 days, up to 12 months.

In addition, we recognize that military spouses often face challenges in finding consistent employment due to frequent relocation for their partners' service. Zscaler invites military spouses to discover flexible, rewarding career opportunities with us, and we recently qualified for the [Military Spouse Employment Partnership](#).



Compensation and Benefits

Zscaler’s competitive compensation and benefits packages support employees’ professional and personal lives. In addition to base pay, employees may be eligible for annual bonuses that are tied to our financial results, as well as long-term equity incentives that vest subject to continued service and performance metrics. Our employee stock purchase plan allows all full-time employees to purchase Zscaler stock at a discount.

Benefits

Supporting the health and well-being of our employees and their families is a top priority. We are committed to providing comprehensive, inclusive benefits that meet the diverse needs of our global team and their families throughout all stages of their lives.

We believe our people should see themselves reflected in their benefits, with the support they need to effectively manage the many dimensions of their lives.

Our packages are designed to be globally competitive and locally relevant, and include the following:

 Health	• Comprehensive health plans • Employee Assistance Program • Mental wellness and mindfulness app
 Financial	• Retirement programs • Life and disability insurance • Global tuition reimbursement • Business travel accident coverage and support
 Work-Life	• Paid time off • Paid parental and family leave • Paid sick and bereavement leave • On-demand learning / development

Well-Being and Mental Health

Zscaler operates in a demanding, high-stakes industry. While we continue to grow and have ambitious goals, we support and encourage employees to take care of themselves and prioritize well-being and mental health. These objectives are reflected in our holistic approach that includes the following:

- Physical: Preventive care and wellness programs and benefits focused on physical activity, nutrition, and self-care.
- Emotional: An enhanced employee assistance program that encourages employees to care for their mental health and provides resources to help manage stress and anxiety, as well as assistance with child and elder care, financial questions, and legal guidance.
- Social: Community programs and mentoring opportunities that cultivate a sense of belonging.

In addition to regularly sharing mental health resources with all employees, we provide managers with training to support their team members. All employees are encouraged to take time off to care for themselves and their families.

Learn more about our comprehensive offerings on the [Zscaler Employee Benefits webpage](#).

Employee Development

We develop employees at every stage of their careers and have made substantial investments in talent development, connecting employees to opportunities to advance their careers and do their best work. This comprehensive approach helps our people grow, rewards performance, and makes us more adept at anticipating customer needs and building for the future.



Leadership Development

Leaders set the tone for our company culture—modeling Zscaler values, cultivating a positive employee experience, and motivating our team to excel. We offer continuous skill-building workshops and resources for all our people managers to support them in successfully leading teams.

Our leadership principles provide a common operating framework as we drive our own company transformation. Our leaders embody them as they guide and develop their teams, and all employees can draw inspiration from them as we adapt and change as a company.

Zscaler's Leadership Principles

- H**ire, develop, and inspire the best
- U**nderstand and innovate with the customer
- M**odel a thoughtful bias for action
- A**ct like an owner
- N**urture a growth mindset

Our leaders benefit from programs tailored to different phases of their journey:

- **Manager Foundations:** We support frontline managers to build essential skills to effectively lead teams at Zscaler.
- **Manager Onboarding:** We support newly hired and promoted managers to learn what's expected of them and how to execute Zscaler's process and practices for managing individuals and teams.
- **Manager Forum:** We enable all people managers globally to build critical leadership skills aligned to our HUMAN Leadership Principles, through continuous skill building and peer-to-peer learning communities.
- **Senior Leaders:** We invest in our senior leaders by bringing them together for networking, collaboration, and problem-solving.

Leaders identified as critical talent have expanded access to development, including one-on-one leadership mentoring, executive coaching, and advanced education.

Training and Development

We provide ample opportunities and resources for career development because employees who are fulfilled in their work take better care of our customers and deliver breakthrough results. Our approach starts by setting new hires up for success, and it continues by offering employees a range of training and development opportunities.

New hires participate in a comprehensive, multi-month onboarding program where they learn about Zscaler's values and culture and how we define success. We are pleased that an average of 92% of new hires responded that they felt like they belonged.

Helping to Address the Cyber Skills Gap

Zscaler has a role to play in making the world more cyber-literate and in preparing students for careers in our industry. Through our [Zscaler Cyber Academy for Students](#), we have partnered with over 550 educational institutions to offer cybersecurity training and heavily discounted certification courses. As of November 2025, more than 49,200 students have received training and certification through this program.

Our training and development programs meet people where they are in their career journey. We offer a variety of learning tools, including structured sales training depending on role, Zscaler product certification, tech talks on cybersecurity developments, self-directed online learning, and resources on leadership best practices. Eligible employees may also receive tuition reimbursement for coursework to enhance their skills. We also offer a mentoring program to all employees which matches mentors and mentees based on their skills and professional interests.

We support internal mobility as one avenue for career development. Our internal career site keeps employees informed of Zscaler job opportunities that might align with their career aspirations and offers a streamlined job application process.

Performance Management

Our integrated approach to performance management reinforces our high-performance culture. Performance reviews aim to fairly assess and reward employees according to their impact and how it was achieved—tied back to our values and leadership principles. Employees and managers have regular check-ins for feedback, along with regular development conversations that provide an opportunity to discuss career aspirations and plans.



Employee Engagement

As we grow, we recognize that sustaining our authentic values and culture, continuing to improve our employees’ experience, and working as one team is critical to our ongoing success. Employee engagement helps us strengthen our workforce and foster support for one another as we achieve our shared objectives.

We are intentional about soliciting feedback and investing in tools to effectively collect and take action on employee sentiment, including through ongoing engagement and pulse surveys aligned with each employee’s journey. Reviewing both quantitative and qualitative input gives us a broad view of the employee experience, keeping our leaders informed of areas for improvement and helping us understand different needs across various demographics and geographies.

95%
of respondents are aligned with Zscaler’s mission

Per our most recent employee survey

92%
of respondents know how their work contributes to Zscaler’s success

In our last global sentiment survey, 93% of employees said they are proud to work at Zscaler. Our unique culture has earned us external recognition, including being named one of Fortune’s Best Workplaces in Technology, Best Workplaces in the Bay Area, among other accolades. We’re proud to have an engaged and motivated workforce that exceeds the survey benchmark for companies in our industry while we remain open to constructive feedback and new ideas.

Zscaler continues to drive engagement and connection among our employees and foster a culture of gratitude. Our internal peer recognition program encourages employees to acknowledge and celebrate their colleagues’ accomplishments.

Workplace Awards

Fortune Best
Workplaces in
Technology

UK Best Large
Workplaces

Fortune Best
Workplaces in
the Bay Area

UK Best Workplaces
for Employee
Development



Community Impact

We believe in the importance of supporting the communities where we operate, and we invest in them by providing volunteer opportunities for our employees and through financial contributions. We are focused on creating secure and resilient communities, equitable access to cybersecurity education, and inclusive cybersecurity career pathways.



Giving Back Program

We refined our community-facing programs to expand employee participation and increase our impact. Over the past year, we:

- Organized more than 50 global events as part of our employee volunteering program
- Further supported volunteering through our community leader program, which supports passionate employees who organize local volunteer events, and our volunteer grants program, which recognizes employee volunteering with funding based on the number of hours served
- Provided year-round flexible donation matches

In India, we supported a variety of corporate social responsibility initiatives, including scaling the impact of STEM education to over 30 schools, launching an additional three cybersecurity resource centers providing expert help on cyber fraud issues to the local community, and establishing a cafe that employs vulnerable communities at the Kempegowda International Airport in Bengaluru. Our volunteers continued our tradition of supporting the environment through local lake cleanup projects.



Helping CXOs Learn and Share Insights

Through Zscaler's [CXO Revolutionaries](#) platform, we connect and empower a global community of C-level technology executives to assist one another in addressing difficult digital transformation and security issues. For the past five years, we have curated exclusive events, roundtables, and panels where CXO pioneers and thought leaders can share their insights and learn from peers. For example, our Women in IT and Security CXO Summit convened women leaders committed to empowering their organizations through digital transformation to share their unique challenges and explore solutions.





Appendix 1: Task Force on Climate-related Financial Disclosures (TCFD) Index

Zscaler follows a comprehensive approach to identifying, assessing, and managing climate-related risks and opportunities across our business. Our approach is informed by the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD), which was established by the Financial Stability Board to provide a voluntary, consistent climate-related financial risk disclosures for use by companies in providing information to investors, lenders, insurers, and other stakeholders. TCFD has since been subsumed by the [International Sustainability Standards Board \(ISSB\)/International Financial Reporting Standards \(IFRS\)](#).

The following index highlights our key public disclosures that align with the recommendations of the TCFD. We are also beginning to voluntarily apply the IFRS Sustainability Disclosure Standard S2, as issued by the ISSB, and are continuing to assess areas for further disclosure. The specific IFRS S2 indicators we report are noted in the index below.

TCFD Recommendation	Related IFRS S2 Indicators	Location or Response
Governance		
a) Describe the board's oversight of climate-related risks and opportunities.	IFRS S2: 6-a, 6-a-i, 6-a-iii, 6-a-iv, 6-a-v	• 2025 Corporate Responsibility Report • Governance > Corporate Governance (p. 8) • Environment > Climate Risk and Opportunity > Climate Risk Governance (p. 22) 2025 CDP Climate Response • 4.1, 4.1.1, 4.1.2, 4.2

TCFD Recommendation	Related IFRS S2 Indicators	Location or Response
b) Describe management’s role in assessing and managing climate-related risks and opportunities.	IFRS S2: 6–b–i, 6–b–ii	2025 Corporate Responsibility Report - Governance > Corporate Governance (p. 8) - Environment > Climate Risk and Opportunity (p. 22) 2025 CDP Climate Response 4.3, 4.3.1, 4.5, 4.5.1
Strategy		
a) Describe the climate-related risks and opportunities the organization has identified over the short, medium and long term.	IFRS S2: 10–a, 10–b, 10–c, 10–d	2025 Corporate Responsibility Report - Environment > Climate Risk and Opportunity Assessment Results (p. 23) 2025 CDP Climate Response 3.1, 3.1.1, 3.1.2, 3.1.3, 3.6, 3.6.1, 3.6.2, 3.6.3
b) Describe the impact of climate-related risks and opportunities on the organization’s businesses, strategy and financial planning.	IFRS S2: 13–a; 13–b	2025 Corporate Responsibility Report - Environment > Climate Risk and Opportunity Assessment Results (p. 23) 2025 CDP Climate Response 2.4, 3.1, 3.1.1, 3.6

TCFD Recommendation	Related IFRS S2 Indicators	Location or Response
c) Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario.	IFRS S2: --	2025 Corporate Responsibility Report - Governance > Risk Management (p. 10) - Environment > Climate Risk and Opportunity (p. 21) - Environment > Climate Risk and Opportunity Assessment Results (p. 22) 2025 CDP Climate Response 5.1, 5.1.1, 5.1.3, 5.1.4
Risk Management		
a) Describe the organization's processes for identifying and assessing climate-related risks.	IFRS S2: 25-a-i, 25-a-ii, 25-a-iii, 25-a-iv, 25-a-v	2025 Corporate Responsibility Report - Governance > Risk Management (p. 10) - Environment > Climate Risk and Opportunity (p. 22) 2025 CDP Climate Response 2.2, 2.2.1, 2.2.2, 2.2.7
b) Describe the organization's processes for managing climate-related risks.	IFRS S2: 14-a; 14-a-i; 14-a-ii, 14-a-iii, 14-a-iv, 14-a-v	2025 Corporate Responsibility Report - Governance > Risk Management (p. 10) - Environment > Our Approach to Managing Environmental Impacts (p. 19) - Environment > Climate Risk and Opportunity (p. 22) 2025 CDP Climate Response 2.2.1, 2.2.2, 2.3, 4.3, 4.3.1, 4.5.1

TCFD Recommendation	Related IFRS S2 Indicators	Location or Response
c) Describe how processes for identifying, assessing and managing climate-related risks are integrated into the organization's overall risk management.	IFRS S2: 25-c	2025 Corporate Responsibility Report - Governance > Risk Management (p. 10) - Environment > Climate Risk and Opportunity (p. 22) 2025 CDP Climate Response 2.2.2, 4.1.2
Metrics and Targets		
a) Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process.	IFRS S2: 25-a-l, 25-a-ii, 29-f-l, 29-g	2025 Corporate Responsibility Report - Overview > Zscaler Highlights (p. 4) - Environment > Our Carbon Footprint (p. 21) 2025 CDP Climate Response 4.5, 4.5.1, 5.10
b) Disclose Scope 1, Scope 2 and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks.	IFRS S2: 29-a-i-1, 29-a-i-2, 29-a-i-3, 29-a-ii, 29-a-iii-1, 29-a-iii-2, 29-a-iii-3, 29-a-iv-1, 29-a-iv-2, 29-a-v, 29-a-vi-1	2025 Corporate Responsibility Report - Environment > Our Approach to Managing Environmental Impacts (p. 19) - Environment > Our Carbon Footprint (p. 21) 2025 CDP Climate Response 7.6, 7.7, 7.8, 7.9, 7.15, 7.16, 7.17, 7.20, 7.22, 7.45, 7.53.1

TCFD Recommendation	Related IFRS S2 Indicators	Location or Response
c) Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets.	IFRS S2: 33-a, 33-b, 33-c, 33-d, 33-e, 33-f, 33-g, 33-h, 34-a, 34- b, 34-c, 34-d, 35, 36-a, 36-b, 36-c, 36-d, 36-e-i, 36-e-ii, 36-e-iii, 36-e-iv	2025 Corporate Responsibility Report - Environment (pp. 17-23) 2025 CDP Climate Response 7.53, 7.53.1, 7.54.3

Appendix 2: Sustainability Accounting Standards Board (SASB) Index

The [SASB Standards](#) identify industry-specific subsets of environmental, social, and governance disclosure topics most relevant to financial performance in 77 industries, categorized pursuant to the [Sustainable Industry Classification System® \(SICS®\)](#). The responsibility for managing these standards is with the [IFRS Foundation](#), a not-for-profit, public interest organization established to develop high-quality, understandable, enforceable and globally accepted accounting and sustainability disclosure standards. Zscaler reports according to the SASB standard for the Software and Information Technology Services Industry.

Topic	Accounting Metric	Category	Unit of Measure	Code	Data / Reference
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-SI-13Oa.1	(1) Total energy consumed: 291,028 GJ (2) and (3). We work with data center providers that draw electricity from the grid and support renewable energy through the purchase of renewable energy certificates (RECs) and virtual power purchase agreements (VPPAs). Through these providers, our hardware infrastructure energy usage is approximately 74.1% renewable. Zscaler matched the remaining nonrenewable energy usage with additional RECs purchases, resulting in 100% renewable energy for our cloud. Note: Data covers January 1, 2024 – December 31, 2024. 2025 Corporate Responsibility Report • Environment (Page 17–23) • Environment Page 2025 CDP Climate Response • 7.29, 7.30.1

Topic	Accounting Metric	Category	Unit of Measure	Code	Data / Reference
Environmental Footprint of Hardware Infrastructure	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Quantitative	Thousand cubic meters (m ³), Percentage (%)	TC-SI-13Oa.2	Zscaler works with data center providers to host our cloud solution. Comprehensive water withdrawal and consumption data is not currently available. 2025 CDP Climate Response 9.1, 9.1.1
	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	n/a	TC-SI-13Oa.3	2025 Corporate Responsibility Report – Environment (Page 17–23)
Data Privacy & Freedom of Expression	Description of policies and practices relating to targeted advertising and user privacy	Discussion and Analysis	n/a	TC-SI-22Oa.1	2025 Corporate Responsibility Report – Governance > Information Security and Privacy (Page 12–14) Privacy Page
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-22Oa.2	Zscaler does not use user information for any purpose other than those stated in our Data Processing Agreement. Zscaler stores only a limited amount of personal data (e.g., IP addresses, URLs, user IDs, and user groups) used to deliver our service. 2025 Corporate Responsibility Report — Governance > Information Security and Privacy (Page 12–14) Privacy Page
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Quantitative	Presentation currency	TC-SI-22Oa.3	Zscaler did not incur any monetary losses as a result of legal proceedings associated with user privacy during the reporting period. Material legal proceedings are disclosed in Zscaler’s public filings.

Topic	Accounting Metric	Category	Unit of Measure	Code	Data / Reference
Data Privacy & Freedom of Expression	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-SI-22Oa.4	(1) 107 in FY25 (2) Not disclosed (3) 0% We did not disclose any user information to agencies. Zscaler is a business-to-business (B2B) service provider. Requests for user information are forwarded to our customers, who manage their users' information. Additional information can be found on our Transparency Report page.
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Discussion and Analysis	n/a	TC-SI-22Oa.5	Zscaler's customers include large multinational organizations with operations throughout the world. Our platform sits inline between the users and content they are trying to access. Zscaler follows all U.S. government regulations concerning embargoed countries.
Data Security	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected	Quantitative	Number, Percentage (%)	TC-SI-23Oa.1	During FY25, Zscaler no breach of the Zscaler platform and any data within it occurred. Material breaches, if any, will be announced on our Trust Portal and disclosed in Zscaler's public filings in accordance with cybersecurity incident disclosure rules from the Securities and Exchange Commission.
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-SI-23Oa.2	• 2025 Corporate Responsibility Report — Governance > Information Security and Privacy (Page 12-14) • Zscaler Certifications

Topic	Accounting Metric	Category	Unit of Measure	Code	Data / Reference
Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that require a work visa	Quantitative	Percentage (%)	TC-SI-33Oa.1	6.1% of our global employees require a work visa in the country where they are employed.
	Employee engagement as a percentage	Quantitative	Percentage (%)	TC-SI-33Oa.2	Based on our employee survey: 95% of respondents are aligned with Zscaler's mission 92% know how their work contributes to Zscaler's success 93% are proud to work at Zscaler
	Percentage of (1) gender and (2) diversity group representation for (a) executive management, (b) non-executive management, (c) technical employees, and (d) all other employees	Quantitative	Percentage (%)	TC-SI-33Oa.3	• 2025 Corporate Responsibility Report – People (Page 29)
Intellectual Property Protection & Competitive Behavior	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Quantitative	Reporting currency	TC-SI-52Oa.1	Zscaler did not incur any monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations during the reporting period. Material legal proceedings, if any, are disclosed in Zscaler's public filings
Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Quantitative	Number, Days	TC-SI-55Oa.1	We are able to meet the 99.999% availability target stated in our Service Level Agreement. Performance issues and disruptions to our service are announced on our Trust Portal .
	Description of business continuity risks related to disruptions of operations	Discussion and Analysis	n/a	TC-SI-55Oa.2	• 2025 Corporate Responsibility Report – Governance > Risk Management (Page 10)

Forward-looking Statements

This report contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our planned products and upgrades, business strategy and plans, and objectives of management for future operations of Zscaler, are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions, and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent filings with the Securities and Exchange Commission. You can locate these reports through our website at <http://ir.zscaler.com> or on the SEC website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as “anticipate,” “believe,” “continues,” “contemplate,” “could,” “estimate,” “expect,” “explore,” “intend,” “likely,” “may,” “plan,” “potential,” “predict,” “project,” “should,” “target,” “goal,” “will,” or “would,” or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this document are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.



For more information, please visit
zscaler.com/corporate-responsibility

For questions, please contact
corporateresponsibility@zscaler.com