kaspersky

Unternehmensprofil: unsere Werte, unser Geschäft, unsere Lösungen und Services

Mai 2026

kaspersky

“Unsere Mission ist einfach – der Aufbau einer sichereren Welt. Wir tun dies, indem wir weltweit führend im Bereich der Cybersicherheit werden. Indem wir Technologie schützen, stellen wir sicher, dass diese frei von Cyberbedrohungen bleibt – und so jedem Menschen nur positive Möglichkeiten bietet.“

„Unendliche Möglichkeiten – für ein sichereres Morgen.“

Eugene Kaspersky, CEO von Kaspersky

Seit fast 30 Jahren dem Aufbau einer sichereren Welt verpflichtet

Kaspersky ist ein internationales Unternehmen für Cybersicherheit und digitale Privatsphäre, das seit fast Jahren eine sicherere digitale Welt aufbaut. In dieser Zeit haben wir unser Portfolio von reiner Endpunktsicherheit hin zu einem umfassenden Schutz von Unternehmen und Verbrauchern entwickelt. Mit einem Team von mehr als 5.700 Fachleuten bauen wir unser Cybersicherheits-Ökosystem weiter aus, mit dem Ziel, alle Sicherheitsanforderungen von Unternehmen und Verbrauchern zu erfüllen, um eine cyberimmune Zukunft zu gewährleisten.

Innovation in der IT-Branche: Das Konzept der Cyber-Immunität

Technologische Meilensteile basierten schon immer auf dem Wunsch nach Innovation. Mit Innovationen geht jedoch das Risiko einher, dass Technologien über ihren beabsichtigten Zweck hinaus missbraucht werden. Auf der Grundlage seiner langjährigen und erfolgreichen Expertise in der Bekämpfung komplexer Cyberkriminalität hat Kaspersky mit seinem Konzept der Cyber-Immunität Pionierarbeit im Bereich der Sicherheit für die IT-Branche geleistet. Cyber-Immunität zielt darauf ab, cyber-physische Systeme zu schaffen, die von Natur aus sicher und geschützt sind, ein Konzept, das KasperskyOS zugrunde liegt.

Eine Milliarde Geräte wurden bis heute[1] durch Kaspersky geschützt

Kaspersky schützt seit fast 30 Jahren Privatanwender und bietet ein entsprechend umfassendes Portfolio an Consumer-Schutzlösungen an, die persönliche Geräte, die Privatsphäre und die digitale Identität zuverlässig schützen. Von preisgekrönter Internet-Sicherheitssoftware über VPN und Passwortverwaltung bis hin zu Parental Control bieten unsere Produkte starken Schutz bei gleichzeitig einfacher und intuitiver Nutzererfahrung. Ob zu Hause oder unterwegs, auf PCs oder Mobilgeräten: wir sorgen dafür, dass sich jeder und jede Einzelne – nicht nur große Organisationen – sicher und selbstbewusst in der digitalen Welt bewegen kann.

[1] Die Zahl basiert auf den Daten des Kaspersky Security Network (KSN) zur automatischen Malware-Analyse und umfasst Datensätze ab 2011, als das System eingeführt wurde.

kaspersky

Wir gewährleisten unterbrechungsfreie Geschäftskontinuität

Kaspersky unterstützt Unternehmen, Betreiber kritischer Infrastrukturen und Behörden dabei, komplexen Bedrohungen immer einen Schritt voraus zu sein. Unsere Lösungen reduzieren Cyberrisiken messbar, sichern einen unterbrechungsfreien Betrieb, ermöglichen eine schnellere Reaktion auf Sicherheitsvorfälle und verringern die Routinearbeit für Teams – unabhängig von der Komplexität der IT-Umgebung. Vom Endpunktschutz bis hin zu Experten-Services bieten wir genau den Schutz, den Unternehmen benötigen. Keine überteuerten Verträge, sondern flexible Sicherheit, die zu den betrieblichen Anforderungen und den tatsächlichen Risikokosten passt.

Sicherheit, die sich dem vorhandenen Ökosystem anpasst, ohne es zu stören

Wir helfen Unternehmen, ihre Geschäftsprozesse zu schützen, Komplexität zu reduzieren und ihre Verteidigung entsprechend den wachsenden Anforderungen zu skalieren. Statt auf einen standardisierten Ansatz zu setzen, sind wir ein echter Partner. Wir verstehen die jeweilige Umgebung und Ressourcen, damit Schutz schnell implementiert und mit dem Unternehmenswachstum flexibel weiterentwickelt werden kann. So werden unnötige Kosten vermieden und bestehende Ressourcen optimal genutzt. Unternehmen erhalten wirksamen Schutz und transparente Kosten, ohne in überflüssige Tools investieren zu müssen.

Bewährte Expertise, auf die Unternehmen vertrauen können

Diese geschäftsorientierte Denkweise wird durch unsere kontinuierliche Bedrohungsforschung unterstützt und vorangetrieben. Über die Hälfte unserer 5.700 Mitarbeiter sind in der Forschung und Entwicklung tätig. Ergänzt wird dies durch langjährige Erfolge in unabhängigen Tests sowie 1.600 Patente weltweit. Deshalb können sich Unternehmen auf unsere Technologien und Innovationen verlassen.

Von kleinen Unternehmen bis hin zu globalen Konzernen skalieren unsere Lösungen mit deren Wachstum. Wir unterstützen Organisationen dabei, Resilienz aufzubauen, die Arbeitsbelastung interner Teams zu reduzieren und Cybersicherheit konsequent an messbaren Geschäftsergebnissen auszurichten.

Threat Intelligence mit echter globaler Reichweite

Kaspersky ist in mehr als 200 Ländern und Territorien tätig und verfügt mit mehr als 100 Millionen Sensoren dort über Echtzeitinformationen aus der ganzen Welt, um seine Nutzer vor Bedrohungen zu schützen, die andere Anbieter möglicherweise übersehen. Wir sind daher die Ersten, die von neuen Bedrohungen erfahren. Unsere globale Abdeckung hilft uns, deren Ausbreitung schnell zu verhindern.

Ein einzigartiges Team von Sicherheitsexperten

Unsere äußerst erfahrenen Expertenteams arbeiten in fünf Expertise Centern rund um die Uhr an der Bekämpfung von Massenangriffen, Malware, zielgerichteten und APT-Angriffen sowie branchen- und infrastrukturspezifischen Bedrohungen, um unsere Kunden zu schützen.

- Das **Kaspersky Global Research and Analysis Team (GReAT)** erforscht und entdeckt die raffiniertesten Bedrohungen (von Duqu, Equation oder Carbanak bis hin zur neuesten Bedrohung Operation Triangulation)
- **Kaspersky Threat Research** forscht im Bereich Anti-Malware und Content Filtering, entwickelt Schlüsseltechnologien zur Bedrohungsabwehr und trägt zu unseren einzigartigen SSDLC[2]- und Secure by Design-Methoden bei.

[2] Secure Software Development Life Cycle

- Das **Kaspersky AI Technology Research Center** befasst sich mit allgemeiner KI-Forschung und KI-gestützter Bedrohungserkennung und Lösungen.
- **Kaspersky Security Services** umfassen MDR, Incident Response, Security Assessments, SOC Consulting und Digital Footprint Intelligence.
- Das **Kaspersky ICS CERT** zeichnet sich im Bereich der industriellen Infrastrukturen aus, führt OT-Bedrohungsanalysen, Schwachstellenforschung und -bewertung durch und arbeitet mit Technologieverbänden und Produktanbietern zusammen, um hohe Sicherheitsstandards für Next-Generation-Technologien zu schaffen.

Die in den Kaspersky Expertise Centern geleistete Arbeit fließt in unsere Lösungen und Services ein, damit unsere Kunden sicher und selbst den raffiniertesten Bedrohungen einen Schritt voraus sind. Weiterführende Informationen zu den Kaspersky Expertise Centern auf unserer offiziellen Website.

Sicherheitsexpertise kombiniert mit der Leistungsfähigkeit von Künstlicher Intelligenz

Künstliche Intelligenz (KI) ist auf dem Vormarsch und revolutioniert viele Branchen – von intelligenten Haushaltsgeräten bis hin zu Robotern in der Produktion und im Geschäftsleben. Kaspersky verfügt über umfangreiche Erfahrungen mit KI und setzt diese schon seit über 20 Jahren zur Lösung spezifischer Probleme ein.

KI-Technologien sind ein integraler Bestandteil unserer Lösungen und Produkte und finden sowohl in Kasperskys eigener Infrastruktur als auch in kundenseitigen Lösungen ihren Platz. Beispielsweise:

- Kaspersky Security Network (KSN) – ein Cloud-Datenverarbeitungszentrum, das globale Bedrohungsdaten sammelt, neue Malware erkennt und dabei hilft, neue Erkennungsmodelle für den späteren Einsatz vor Ort zu erstellen, die in mehrere Kaspersky-Produkte integriert sind.
- Kaspersky Industrial CyberSecurity (KICS) und Machine Learning for Anomaly Detection (MLAD) nutzen KI-Algorithmen, um indirekte Angriffsindikatoren und subtile Aktivitätsanomalien in hochspezifischen industriellen Umgebungen zu erkennen.
- Die Managed Detection and Response (MDR)-Plattform wird durch den KI-basierten Autoanalysten unterstützt, der mit Alarmen des SOC-Teams gespeist wird, um diese später automatisch zu verarbeiten und die SOC-Analysten von einem erheblichen Teil manueller Arbeit zu entlasten.

Wir sind zum derzeitigen Stand der Entwicklung von KI überzeugt davon, dass die effektivsten Lösungen entstehen, wenn Menschen und Maschinen zusammenarbeiten und ihre Stärken gegenseitig maximieren. Unser Team im Kaspersky AI Technology Research Center arbeitet seit fast zwei Jahrzehnten mit KI in der Cybersicherheit und mit ethischer KI, um ein breites Spektrum an Bedrohungen zu entdecken und zu bekämpfen. Ihre Arbeit ist der Beweis dafür, dass die Verbindung von KI-Fähigkeiten mit menschlichem Fachwissen und umfassenden Bedrohungsdaten aus Big Data die effektivste und zuverlässigste Sicherheit schafft.

Höchste Qualität bestätigt durch zahlreiche Tests und Auszeichnungen

Unsere Produkte werden regelmäßig externen Überprüfungen und Tests unterzogen und erhalten die höchsten Auszeichnungen und Anerkennungen. Laut AV-Comparatives Security Survey 2025 ist

Kaspersky die beliebteste Desktop-Sicherheitslösung in Europa, Asien, Mittel- und Südamerika und wurde als der Anbieter „der das Jahr geprägt hat“ („who shaped the year“) im IDC-Bericht „Worldwide Consumer Digital Life Protection Market Shares“[3] aufgeführt. Mit über 950[4] Branchenauszeichnungen für seine Sicherheitslösungen ist Kaspersky zudem einer der anerkanntesten Sicherheitsanbieter auf dem Markt. Unsere Technologien und Prozesse werden von einigen der weltweit angesehensten Organisationen umfassend geprüft und zertifiziert, um die beste Sicherheit für unsere Kunden zu gewährleisten.

Weitere Informationen über unabhängige Bewertungen und Zertifizierungen

Kaspersky arbeitet kontinuierlich mit weltweit anerkannten Organisationen zusammen, um seine internen Prozesse unabhängig überprüfen zu lassen, darunter:

- Service Organization Control (SOC 2) for Service Organizations-Audits durchläuft Kaspersky seit 2019. Im Jahr 2025 erneuerte Kaspersky außerdem ein umfassendes SOC-Typ-2-Audit, das die Wirksamkeit der zum Schutz des Prozesses der Entwicklung von Antiviren-Datenbanken implementierten Kontrollen bestätigt.
- Die Zertifizierung nach ISO/IEC 27001:2013, dem internationalen Standard, der Best Practices für Informationssicherheits-Managementsysteme festlegt, wurde von Kaspersky im Jahr 2020 erlangt. Eine Re-Zertifizierung mit erweitertem Geltungsbereich fand im Jahr 2025 statt.

Globale Transparenzinitiative: Wir sind transparent in unserer Arbeitsweise und wie wir Verbraucher und Unternehmen schützen

Kaspersky ist das erste Cybersicherheitsunternehmen, das seinen Quellcode öffentlich zur externen Überprüfung bereitstellt und Kunden sowie Partnern seine Software Bill of Materials (SBOM) zur Verfügung stellt. Um das Vertrauen in das hohe Niveau unseres Datenschutzes zu stärken, ermöglicht es unser internationales Netzwerk von Transparenzzentren Interessenvertretern, sich über unsere internen Prozesse und Datenmanagementpraktiken zu informieren.

Weitere Informationen zur Globalen Transparenzinitiative

Kaspersky verpflichtet sich, seine Kunden vor Cyberbedrohungen zu schützen, unabhängig von deren Ursprung oder Zweck. Die Globale Transparenzinitiative (GTI) des Unternehmens hat zum Ziel, die breitere Informationssicherheitsgemeinschaft und andere Interessengruppen in die Validierung und Verifizierung der Vertrauenswürdigkeit seiner Produkte, internen Prozesse und Geschäftsabläufe einzubeziehen. Kaspersky führt zudem zusätzliche Mechanismen der Rechenschaftspflicht ein, über die das Unternehmen weiter nachweist, dass es alle Sicherheitsprobleme umgehend und gründlich angeht. Weitere Informationen zur Geschichte der Globalen Transparenzinitiative und ihrer Expansion weltweit unter https://gti.kaspersky.com/de.

Die GTI von Kaspersky umfasst eine Reihe umsetzbarer und konkreter Maßnahmen:

- **Externe Überprüfung** des Quellcodes des Unternehmens, Softwareupdates und Bedrohungserkennungsregeln
- **Unabhängige Überprüfung** der sicheren Entwicklung der Lifecycle-Prozesse sowie der Strategien zur Risikominimierung in der Software-Entwicklungskette

[3] IDC Worldwide Consumer Digital Life Protection Market Shares 2024 (Juni 2025)
[4] Die Zahl umfasst unabhängige Testergebnisse von Unternehmens- und Verbraucherprodukten im Zeitraum 2013-2025.

- **Verlagerung der cyberbedrohungsbezogenen Datenspeicherung und -verarbeitung in die Schweiz** für Kunden in Europa, Nord- und Lateinamerika, im Mittleren Osten sowie in mehreren Ländern im asiatisch-pazifischen Raum.
- **Globale Transparenzzentren weltweit,** um Sicherheitsbedenken zusammen mit Kunden, vertrauenswürdigen Partnern und Regierungsvertretern anzugehen. Die Kaspersky Transparenzzentren befinden sich in den Regionen META, Asien-Pazifik, Europa und Lateinamerika.
- **Höhere Prämien für das Bug Bounty Programm** im Rahmen des Vulnerability Disclosure-Programms von Kaspersky von bis zu 100.000 US-Dollar für schwerwiegende Schwachstellen. Seit 2022 betreibt Kaspersky sein öffentliches Bug-Bounty-Programm auf der Yogosha-Plattform. Außerdem unterstützen wir das Disclose.io-Framework, das Sicherheitsforschern, die sich über negative rechtliche Folgen ihrer Entdeckungen Sorgen machen, einen Safe Harbor bietet.
- **Transparenz des Unternehmens in seiner Responsible Vulnerability Disclosure** durch die Veröffentlichung seiner ethischen Grundsätze.
- **Transparenzberichte**, in denen die Anzahl der Anfragen von Strafverfolgungs- und Regierungsbehörden nach Informationen über Nutzerdaten, Fachwissen und technische Informationen zur Untersuchung von Bedrohungen offengelegt wird.
- **Start des Cyber Capacity Building Programs**, eines speziellen Schulungskurses (auch online verfügbar) zur Bewertung der Produktsicherheit für mehr Sicherheit und Cyber-Resilienz des IKT-Ökosystems.

Bildung und Zusammenarbeit für ein sichereres digitales Zeitalter

Kaspersky klärt seine Nutzer über die sich entwickelnde Cyberbedrohungslandschaft auf und spricht auf verständliche Weise über komplexe digitale Themen. Das Unternehmen arbeitet daran, die Online-Sicherheit von Kindern zu verbessern und unterstützt die Entwicklung junger Talente, indem es zur internationalen IT-Community beiträgt. Kaspersky leitet zudem weltweite Verbände und gemeinsame Projekte zum Schutz Bedürftiger – ganz im Sinne der Unternehmensmission „Building a safer world“.

Weitere Informationen zu unserer Rolle in der weltweiten IT-Sicherheits-Community

Zusammenarbeit ist der effektivste Weg, um eine sicherere Welt aufzubauen und Cyberkriminelle zu bekämpfen. Wir glauben, dass es keine Grenzen für Sicherheit gibt. Daher teilen wir unsere Expertise, unser Wissen und unsere technischen Erkenntnisse mit der weltweiten Sicherheitsgemeinschaft. Unser Unternehmen hat an Untersuchungen mit Adobe, AlienVault Labs, Novetta, CrowdStrike, OpenDNS und weiteren teilgenommen.

Wir sind stolz darauf, mit globalen IT-Sicherheitsanbietern, internationalen Organisationen und nationalen sowie regionalen Strafverfolgungsbehörden auf der ganzen Welt bei der Bekämpfung der Internetkriminalität zusammenzuarbeiten.

Zusammen mit Strafverfolgungsbehörden und CERTs weltweit, kooperiert Kaspersky mit INTERPOL zur gemeinsamen Bekämpfung von Internetkriminalität. Das Unternehmen bietet der Organisation Personalunterstützung, Schulungen und Bedrohungsdaten in Bezug auf die neuesten Cyberkriminalitätsaktivitäten. Konkret haben Kaspersky-Forscher seit 2019 Schulungen für INTERPOL-Vollzugsbeamte durchgeführt, darunter mehr als 10 Cybersecurity-Trainingsveranstaltungen.

Um die globalen Bemühungen zur Bekämpfung von Cyberkriminalität weiter zu stärken, haben Kaspersky und AFRIPOL eine Kooperationsvereinbarung zur Prävention und Bekämpfung von Cyberkriminalität

unterzeichnet. Kaspersky und AFRIPOL blicken auf eine lange Geschichte gemeinsamer Kooperationsprojekte zurück, in der die beiden Organisationen aktiv zur Bewertung der afrikanischen Bedrohungslandschaft und zur Bekämpfung der Cyberkriminalität beigetragen haben, speziell zur Africa Cyber Surge Operation und Africa Cyber Surge Operation II. Im Jahr 2026 führte Kaspersky im Rahmen einer gemeinsamen Initiative mit AFRIPOL Schulungen zur Cybersicherheit für Vertreter der Strafverfolgungsbehörden aus 23 afrikanischen Ländern durch, in denen die Grundlagen der Aktivitäten eines Security Operations Center (SOC) und fortgeschrittene Techniken zur Bedrohungsanalyse erläutert wurden.

Kaspersky ist zudem Mitglied in Initiativen und Organisationen wie Securing Smart Cities, dem Industrial Internet Consortium, AUTOSAR, International Telecommunication Union und International Organization for Standardization. Wir sind Gründungsmitglied der Coalition Against Stalkerware und der NoMoreRansom-Initiative und nehmen als Partner am Genfer Dialog teil – einer Gruppe von Interessenvertretern, die einen internationalen Prozess und Dialog über die Sicherheit digitaler Produkte führt. Wir nehmen an gemeinsamen Untersuchungen von Cyberbedrohungen teil und führen Schulungen für Cybersicherheitsspezialisten und internationale Polizeiorganisationen durch. So hat beispielsweise die Zusammenarbeit zwischen der niederländischen Polizei und Kaspersky zur Verhaftung der hinter den Coinvault-Ransomware-Attacken stehenden Verdächtigen geführt.

Kaspersky beteiligt sich auch proaktiv an UN-Initiativen wie Global Digital Compact, der Open-Ended Working Group on the Security and Use of ICT und dem Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes. Kaspersky nahm zudem häufig am Internet Governance Forum (IGF) unter der Schirmherrschaft der Vereinten Nationen teil, wo das Unternehmen seine ethischen Prinzipien für die Nutzung von KI in der Cybersicherheit vorstellte und Leitfäden für die sichere Entwicklung und den Einsatz von KI-Systemen vorschlug.

Im Jahr 2025 unterzeichnete Kaspersky ein Kooperationsabkommen mit JUPOL, um die Cybersicherheitskapazitäten der spanischen Polizei zu stärken. Die Partnerschaft konzentriert sich auf die Verbesserung der Fähigkeiten der Beamten durch Schulungen, die Optimierung ihrer Reaktionsfähigkeit auf Cyberkriminalität und die Förderung der Zusammenarbeit zwischen öffentlichem und privatem Sektor.

Weitere Informationen zu unseren Bildungsinitiativen

Wir sind davon überzeugt, dass die Ermutigung zum Dialog und die Einführung von Bildungsprogrammen für die internationale Zusammenarbeit im Kampf gegen Cyberkriminalität essenziell sind. Daher betreiben wir die Kaspersky Academy: ein internationales Bildungsprojekt, das 2010 ins Leben gerufen wurde. Im Rahmen dieses Programms fördern wir das Wissen über Cybersicherheit weltweit, indem wir junge Talente in der IT fördern und zur Entwicklung erstklassiger Bildungsprogramme für Cybersicherheit beitragen.

Um jungen Talenten das breite Wissen über berufliche Laufbahnen im Bereich Cybersicherheit zu vermitteln und ihre zukünftige IT-Karriere anschaulicher zu gestalten, hat Kaspersky außerdem das Projekt Tech Valley ins Leben gerufen, das sich auf erfahrene Wissenschaftler und Studenten konzentriert. 2023 hat Kaspersky Academy die Kaspersky Academy Alliance ins Leben gerufen, ein spezielles Programm für Universitäten, das die Cybersecurity-Expertise und die neuesten Kaspersky-Technologien in die Lehre integriert, um die akademischen Leistungen der Studenten zu verbessern.

Im gleichen Jahr kündigte Kaspersky außerdem sein Projekt „Kids‘ Cyber Resilience“ an. Das Ziel dieses Projekts besteht darin, einen kollaborativen und proaktiven Ansatz für Online-Sicherheit zu etablieren und Kindern dabei zu helfen, mit Stress umzugehen und mit Herausforderungen in der digitalen Umgebung umzugehen. 2024 weitete Kaspersky diese Initiative über Vietnam hinaus auf den Nahen Osten und die GUS-Länder aus. Im selben Jahr veröffentlichte Kaspersky für Kinder im Alter von 5-12 Jahren das Buch "Cybersecurity Alphabet", in dem sie neue Technologien kennenlernen, die wichtigsten Regeln der Cyber-

Hygiene erfahren, herausfinden, wie sie Online-Bedrohungen vermeiden und die Tricks von Betrügern erkennen können. Darüber hinaus kündigte Kaspersky im Jahr 2025 die Eröffnung seines Cyber Research Centers im KidZania in Santa Fe an, um junge Nutzer über die Bedeutung digitaler Sicherheit aufzuklären.

Neben der Aufklärung der Kinder werden Eltern und Pädagogen mit Wissen und Tools ausgestattet, mit denen sie Online-Probleme wie Stressquellen oder Unbehagen erkennen sowie potenzielle Cyberrisiken verringern können. Weiterhin bietet das Projekt Unterstützung für diejenigen, die von Cyber-Mobbing und anderen Formen negativer Online-Erfahrungen betroffen sind. Die Kaspersky-Experten tragen auch mit Lernmaterialien für Junior High Schools bei.

Darüber hinaus führt das Unternehmen Kaspersky Expert Trainings durch, die Fachleute helfen, effektive Strategien zur Erkennung und Abwehr von Bedrohungen zu erlernen, um die sich ständig weiter entwickelnden Gefahren der heutigen Cyber-Realität zu bekämpfen.

Weitere Informationen zu unseren sozialen Projekten

In unserer Bemühung, eine sicherere Zukunft zu schaffen, sorgen wir uns nicht nur digital um das Wohlergehen der Welt. Zu den Kernbereiche der nachhaltigen Entwicklung von Kaspersky gehören die Umweltverträglichkeit unserer Infrastruktur, unserer Geschäftsaktivitäten und Produkte, Mitarbeiterpflege, Inklusion und die Verfügbarkeit von Technologien. Das Unternehmen veröffentlicht seine Nachhaltigkeitsberichte seit 2023 und erstellt sie nach den internationalen GRI- und SASB-Standards. Der neueste Bericht ist unter https://esg.kaspersky.com/en/ verfügbar.

Kaspersky hat die Online-Community ‚Women in Cybersecurity' gegründet, die dazu beiträgt, die Karriere von Frauen, die in die Cybersicherheitsbranche einsteigen, und von Frauen, die bereits in diesem Bereich tätig sind, zu beschleunigen. Darüber hinaus haben wir das digitale Projekt ‚Empower Women' initiiert, mit dem Ziel, durch Wissensaustausch weitere Brücken zwischen Frauen und Männern auf allen Ebenen des Unternehmens zu schlagen. Dies trägt dazu bei, ein Arbeitsumfeld zu schaffen, in dem alle ihr volles Potenzial entfalten können – unabhängig vom Geschlecht.

Im Jahr 2025 startete Kaspersky „Future You in Tech", eine neue Initiative zur Förderung der nächsten Generation von Frauen im Technologiebereich. Das Projekt richtet sich an junge Frauen, die berufliche Perspektiven erkunden, und hilft diesen, den Cybersicherheitssektor, seine Karrieremöglichkeiten und passende Positionen für ihre Interessen und Stärken zu verstehen.

Kaspersky setzt sich seit langem für die Bekämpfung von digitaler Gewalt und technologiegestütztem Missbrauch ein. Im Jahr 2019 führte das Unternehmen einen Spyware-Schutz in seine Android-App ein und war damit das erste Unternehmen, das seinen Nutzern einen robusten Schutz gegen Stalkerware – kommerzielle Spionageprogramme, die zwar als legal gelten, jedoch zur heimlichen Überwachung und Verfolgung der Geräte eines Partners verwendet werden können und häufig zu häuslicher Gewalt führen – bot. Im selben Jahr gründete Kaspersky die Koalition gegen Stalkerware zusammen mit weiteren IT-Sicherheitsunternehmen, Nichtregierungsorganisationen, Forschungseinrichtungen und Strafverfolgungsbehörden, um gemeinsam gegen intrusive Software und digitalen Missbrauch vorzugehen. Die zu Beginn zehn Mitglieder umfassende Koalition vereint heute mehr als 40 Geschäftspartner im Kampf gegen Cyberstalking und wird von INTERPOL unterstützt. Darüber hinaus unterstützt Kaspersky Non-Profit Organisationen, die mit Betroffenen häuslichen Missbrauchs arbeiten.

Im Rahmen seines Engagements zur Bekämpfung von Online- und Offline-Stalking integrierte Kaspersky kürzlich die Funktion „Who's Spying on Me" in seine Android-Apps. Diese Innovation erkennt nicht nur Stalkerware, sondern identifiziert auch verdächtige Bluetooth-Geräte, die potenziell für Offline-Tracking verwendet werden können. Durch diese Art von Erweiterungen seiner Schutzfunktionen unterstützt Kaspersky seine Nutzer immer mehr die Kontrolle über ihre eigene Sicherheit und Privatsphäre zu übernehmen.

2024 startete Kaspersky einen Anti-Stalking Awareness Guide – eine neue Initiative, die Psychologen und Betroffene von Stalking einbezieht. Durch die Kombination von Fachwissen aus verschiedenen Disziplinen hilft dieser Leitfaden den Anwendern nicht nur, Anzeichen von Stalking zu erkennen und Schutzmaßnahmen zu ergreifen, sondern gibt auch den Stimmen von Überlebenden Raum und inspiriert andere dazu, ihr Gefühl von Sicherheit und Kontrolle wiederzuerlangen.

Kaspersky war Partner des EU-weiten Projekts „DeStalk“ mit einer Laufzeit von 2021-2023, das die Europäische Kommission mit ihrem Programm „Rechte, Gleichstellung und Unionsbürgerschaft“ unterstützte. DeStalk befasst sich mit den Themen Cybergewalt und Stalkerware, die neue, weit verbreitete und versteckte Formen geschlechtsspezifischer Online-Gewalt darstellen.