Docusign Envelope ID: CFCD5CD7-D495-86F2-829D-57AAFC9C4778

Palo Alto Networks Human Trafficking & Anti-Slavery Statement

Introduction

At Palo Alto Networks, our vision is a world where each day is safer and more secure than the one before.

Palo Alto Networks is committed to ensuring that our supply chain is free from human trafficking or modern slavery. We believe in upholding the human rights of all workers and treating workers with dignity and respect. We do not tolerate or accept use of forced or child labor in our supply chain. We have implemented a number of policies in support of the protection of human rights, which can be found on our website here. We have also implemented numerous internal policies at the global and local level, including local work rules, ensuring our employees know of our commitments and the various avenues available to them to raise concerns.

The *United Kingdom Modern Slavery Act 2015* requires disclosure of information relating to applicable business efforts to address the risks of modern slavery (including forced labor and human trafficking) in their operations and supply chains. This statement is made on behalf of the specific subsidiaries of Palo Alto Networks, Inc. that are subject to modern slavery disclosure obligations (the "Reporting Entities").[1] While modern slavery compliance programs are centrally managed by Palo Alto Networks, Inc. on a global basis, this statement outlines the collective efforts of the Reporting Entities during the fiscal year ended July 31, 2025. For the purposes of this statement, 'Palo Alto Networks,' 'the Company,' 'we,' or 'our' refer collectively to Palo Alto Networks, Inc. and its consolidated subsidiaries.

Structure, operations, and supply chain

Palo Alto Networks Inc. was incorporated in 2005 and is headquartered in Santa Clara, CA. As of the end of the fiscal year, which ended on July 31, 2025, the Company had approximately 16,068 employees located in over 30 countries (including 450 employed in the United Kingdom). We provide cybersecurity software services and industry leading lines of security hardware that empower enterprises, organizations, service providers, and government entities to protect themselves against today's most sophisticated cyber threats. Our cybersecurity platforms and services help secure enterprise users, networks, clouds, and endpoints by delivering comprehensive cybersecurity backed by industry leading artificial intelligence and automation. We are a leading provider of zero trust solutions, starting with next-generation zero trust network access to secure today's remote hybrid workforces and extending to securing all users, applications, and infrastructure with zero trust principles. Our security solutions are designed to reduce customers' total cost of ownership by improving operational efficiency and eliminating the need for siloed point products.

Palo Alto Networks, Inc. and its subsidiaries operate worldwide and are collectively known as Palo Alto Networks. A complete list of subsidiaries, as of the end of the fiscal year ended July 31, 2025, can be found in Exhibit 21.1 to Palo Alto Networks, Inc.'s Form 10-K, filed with the US Securities and Exchange Commission on August 29, 2025.

Palo Alto Networks is a well-integrated business. The same practices and procedures regarding responsible business and core ethics and compliance requirements apply to all global subsidiaries, affiliates, and related entities.

Palo Alto Networks outsources the manufacturing of our products to various manufacturing partners, including our electronics manufacturing services provider ("EMS provider") and original design manufacturers. Our providers assemble our products using design specifications, quality assurance programs, and standards that we establish, and procure components and assemble our products based on our demand forecasts. Palo Alto

[1] The Reporting Entities covered by this statement pursuant to Section 54(1) of the UK Modern Slavery Act 2015 include: Palo Alto Networks (UK) Limited, Palo Alto Networks (UK Holding 1) Limited, Palo Alto Networks (UK Holding 2) Limited, and Palo Alto Networks FS International Limited.

Docusign Envelope ID: CFCD5CD7-D495-86F2-829D-57AAFC9C4778

Networks and our partners source component parts within our hardware products from more than 300 suppliers within 30 countries across Asia, North America, and Europe. Our operations also include design and product development, supply chain management, marketing, sales, customer support, and administrative operations.

Risks of modern slavery and actions taken to assess and reduce risks

We recognize that a global supply chain starting at mineral extraction and ending with product assembly and repair presents modern slavery and forced labor risks. We believe these risks predominate in mineral extractive industries and with manufacturing suppliers operating in countries where a high volume of migrant labor is utilized and where there is potentially a lack of adequate legal protections for migrant workers. In our own operations, we believe the risks of modern slavery and forced labor are predominantly associated with third-party service providers who support our office operations, including facility, custodial, and security staff. The risks associated with the use of such third-party service providers likewise primarily revolve around the potential use of a migrant workforce where knowledge of employment rights may be lower and therefore the risks of forced labor may be higher.

To help assess and mitigate the risks inherent in our supply chain, Palo Alto Networks has implemented a Conflict Minerals Policy and attendant Conflict Minerals program, using leading industry developed tools from the Responsible Minerals Initiative to help track specific minerals from the mine to the smelter or refiner. We conduct annual surveys to minimize risk associated with use of components from regions with highest known risks of modern slavery and forced labor. We also conduct risk-based due diligence and utilize risk monitoring tools designed to notify us of credible public allegations and concerns relating to modern slavery and forced labor use by companies within our supply chain. We require suppliers to certify their adherence to and fidelity with Palo Alto Networks' Global Supplier Code of Conduct. Where applicable, our suppliers must also verify their compliance with the Responsible Business Alliance (the "RBA") Code of Conduct. We work to effectuate positive change within our supply chain by using relevant information and certifications to encourage improvements and remediation of behavior that falls short of our expectations, removing vendors and suppliers who fail to meet our high-standards and expectations as necessary.

Palo Alto Networks supports the United Nations Global Compact and the protection of internationally proclaimed human rights and labor standards. In furtherance of our commitment, Palo Alto Networks is an Affiliate Member of the RBA and adheres to the RBA Code of Conduct. Our Global Supplier Code of Conduct requires our supply chain partners to support this initiative and requires our suppliers to:

1) strictly prohibit human trafficking;
2) ensure all employment or services are freely chosen;
3) strictly prohibit child labor;
4) ensure workweeks are not excessive and are in compliance with local law;
5) pay compensation in accordance with local law;
6) ensure there is no harsh or inhumane treatment of its workers;
7) ensure a workforce free of harassment and unlawful discrimination;
8) provide freedom of association for all workers, in conformance with local law;
9) implement and maintain an occupational health and safety program; and
10) implement a grievance mechanism to allow workers to report concerns.

Palo Alto Networks employees receive annual training on our Code of Conduct. The training establishes and makes clear our expectations that all employees comply with the Code of Conduct, which includes relevant provisions on protection of human rights and treatment of workers, including strict prohibition on modern slavery and forced labor. In addition, employees involved in hardware sourcing receive regular periodic training to maintain and enhance their knowledge of applicable global regulations and best practices. This may include,

Docusign Envelope ID: CFCD5CD7-D495-86F2-829D-57AAFC9C4778

but is not limited to, attending webinars, roundtables, and conferences, or reviewing internal and external training materials.

Due diligence processes and remediation

Palo Alto Networks takes a risk-based approach to due diligence, focusing resources on sector and geographic specific risks, utilizing due diligence and continuous risk monitoring tools to help identify red flags relating to vendors and suppliers, or their failure to abide by their modern slavery and forced labor obligations. In addition, we require selected direct suppliers, prioritized based on our risk assessment, to complete an annual questionnaire and to disclose certain labour practices and policies.

Palo Alto Networks maintains a culture of open communication and encourages anyone with a good-faith concern to speak up without fear of retaliation. We have implemented multiple internal and external communication channels to make it convenient for employees, business partners, and members of our community to ask questions, provide feedback, or report concerns. As outlined above, we require the same from our suppliers. Palo Alto Networks is committed to investigating any credible report of potential modern slavery and forced labor or other applicable Code of Conduct violations in a fair, consistent, comprehensive, and objective manner. In line with our core beliefs, we confirm that we will take all appropriate and necessary steps to rectify any confirmed incidences of modern slavery and forced labor in our operations or supply chains.

Assessing the effectiveness of actions taken to address modern slavery risks

During this reporting period, Palo Alto Networks assessed the effectiveness of our actions through the information collected in its annual partner surveys, conversations with suppliers, and the tools we utilized to conduct due diligence and assess risk.

Approval

This Human Trafficking & Anti-Slavery Statement was adopted and approved by the Board of Directors of Palo Alto Networks (UK) Limited on July 6, 2026.

Signed by:
5052DCC647BE44C...

Signed for and on behalf of Palo Alto Networks (UK) Limited

Kevin Espinola

Director, Palo Alto Networks (UK) Limited

This Human Trafficking & Anti-Slavery Statement was adopted and approved by the Board of Directors of Palo Alto Networks (UK Holding 1) Limited on July 6, 2026.

Signed by:
5052DCC647BE44C...

Signed for and on behalf of Palo Alto Networks (UK Holding 1) Limited

Kevin Espinola

Director, Palo Alto Networks (UK Holding 1) Limited

Docusign Envelope ID: CFCD5CD7-D495-86F2-829D-57AAFC9C4778

This Human Trafficking & Anti-Slavery Statement was adopted and approved by the Board of Directors of Palo Alto Networks (UK Holding 2) Limited on July 6, 2026.

Signed by:
5052DCC647BE44C...

Signed for and on behalf of Palo Alto Networks (UK Holding 2) Limited

Kevin Espinola

Director, Palo Alto Networks (UK Holding 2) Limited

This Human Trafficking & Anti-Slavery Statement was adopted and approved by the Board of Directors of Palo Alto Networks FS International Limited on July 6, 2026.

Signed by:
5052DCC647BE44C...

Signed for and on behalf of Palo Alto Networks FS International Limited

Kevin Espinola

Director, Palo Alto Networks FS International Limited

Docusign Envelope ID: A8E0F3D7-F122-8DFE-83B3-625428BADFA2

Palo Alto Networks Human Trafficking & Anti-Slavery Statement

Introduction

At Palo Alto Networks, our vision is a world where each day is safer and more secure than the one before.

Palo Alto Networks is committed to ensuring that our supply chain is free from human trafficking or modern slavery. We believe in upholding the human rights of all workers and treating workers with dignity and respect. We do not tolerate or accept use of forced or child labor in our supply chain. We have implemented a number of policies in support of the protection of human rights, which can be found on our website here. We have also implemented numerous internal policies at the global and local level, including local work rules, ensuring our employees know of our commitments and the various avenues available to them to raise concerns.

The Australian *Modern Slavery Act 2018* requires disclosure of information relating to applicable business efforts to address the risks of modern slavery (including forced labor and human trafficking) in their operations and supply chains. This statement is made by Palo Alto Networks, Inc. on behalf of its Australian subsidiary Palo Alto Networks (Australia) Pty Ltd that is subject to modern slavery disclosure obligations (the "Reporting Entity").[1] While modern slavery compliance programs are centrally managed by Palo Alto Networks, Inc. on a global basis, this statement outlines the collective efforts of Palo Alto Networks, Inc. and the Reporting Entity during the fiscal year ended July 31, 2025. For the purposes of this statement, 'Palo Alto Networks,' 'the Company,' 'we,' or 'our' refer collectively to Palo Alto Networks, Inc. and its consolidated subsidiaries.

Structure, operations, and supply chain

Palo Alto Networks Inc. was incorporated in 2005 and is headquartered in Santa Clara, CA. As of the end of the fiscal year, which ended on July 31, 2025, the Company had 16,068 employees located in over 30 countries (including 370 employed in Australia). We provide cybersecurity software services and industry leading lines of security hardware that empower enterprises, organizations, service providers, and government entities to protect themselves against today's most sophisticated cyber threats. Our cybersecurity platforms and services help secure enterprise users, networks, clouds, and endpoints by delivering comprehensive cybersecurity backed by industry leading artificial intelligence and automation. We are a leading provider of zero trust solutions, starting with next-generation zero trust network access to secure today's remote hybrid workforces and extending to securing all users, applications, and infrastructure with zero trust principles. Our security solutions are designed to reduce customers' total cost of ownership by improving operational efficiency and eliminating the need for siloed point products.

Palo Alto Networks, Inc. and its subsidiaries operate worldwide and are collectively known as Palo Alto Networks. A complete list of subsidiaries, as of the end of the fiscal year ended July 31, 2025, can be found in Exhibit 21.1 to Palo Alto Networks, Inc.'s Form 10-K, filed with the US Securities and Exchange Commission on August 29, 2025.

Palo Alto Networks outsources the manufacturing of our products to various manufacturing partners, including our electronics manufacturing services provider ("EMS provider") and original design manufacturers. Our providers assemble our products using design specifications, quality assurance programs, and standards that we establish, and procure components and assemble our products based on our demand forecasts. Palo Alto Networks and our partners source component parts within our hardware products from more than 300 suppliers within 30 countries across Asia, North America, and Europe. Our operations also include design and product development, supply chain management, marketing, sales, customer support, and administrative operations.

[1] The Reporting Entity covered by this statement pursuant to the Commonwealth *Modern Slavery Act 2018* is Palo Alto Networks (Australia) Pty Ltd. Palo Alto Networks (Australia) Pty Ltd has one subsidiary - Sinefa Pty Ltd. Sinefa Pty Ltd is currently largely inactive.

Docusign Envelope ID: A8E0F3D7-F122-8DFE-83B3-625428BADFA2

Risks of modern slavery and actions taken to assess and reduce risks

We recognize that a global supply chain starting at mineral extraction and ending with product assembly and repair presents modern slavery risks. We believe these risks predominate in mineral extractive industries and with manufacturing suppliers operating in countries where a high volume of migrant labor is utilized and where there is potentially a lack of adequate legal protections for workers. In our own operations, we believe the risks of modern slavery are predominantly associated with third-party service providers who support our office operations, including facility, custodial, and security staff. The risks associated with the use of such third-party service providers likewise primarily revolve around the potential use of a migrant workforce where knowledge of employment rights may be lower and therefore the risks of modern slavery may be higher.

To help assess and mitigate the risks inherent in our supply chain, Palo Alto Networks has implemented a Conflict Minerals Policy and attendant Conflict Minerals program, using leading industry developed tools from the Responsible Minerals Initiative to help track specific minerals from the mine to the smelter or refiner. We conduct annual surveys to minimize risk associated with use of components from regions with highest known risks of modern slavery. We also conduct risk-based due diligence and utilize risk monitoring tools designed to notify us of credible public allegations and concerns relating to modern slavery use by companies within our supply chain. We require suppliers to certify their adherence to and fidelity with Palo Alto Networks' Global Supplier Code of Conduct. Where applicable, our suppliers must also verify their compliance with the Responsible Business Alliance (the "RBA") Code of Conduct. We work to effectuate positive change within our supply chain by using relevant information and certifications to encourage improvements and remediation of behavior that falls short of our expectations, removing vendors and suppliers who fail to meet our high-standards and expectations as necessary.

Palo Alto Networks supports the United Nations Global Compact and the protection of internationally proclaimed human rights and labor standards. In furtherance of our commitment, Palo Alto Networks is an Affiliate Member of the RBA and adheres to the RBA Code of Conduct. Our Global Supplier Code of Conduct requires our supply chain partners to support this initiative and requires our suppliers to:

1) strictly prohibit human trafficking;
2) ensure all employment or services are freely chosen;
3) strictly prohibit child labor;
4) ensure workweeks are not excessive and are in compliance with local law;
5) pay compensation in accordance with local law;
6) ensure there is no harsh or inhumane treatment of its workers;
7) ensure a workforce free of harassment and unlawful discrimination;
8) provide freedom of association for all workers, in conformance with local law;
9) implement and maintain an occupational health and safety program; and
10) implement a grievance mechanism to allow workers to report concerns.

Palo Alto Networks' employees receive annual training on our Code of Conduct. The training establishes and makes clear our expectations that all employees comply with the Code of Conduct, which includes relevant provisions on protection of human rights and treatment of workers, including strict prohibition on modern slavery in our operations and supply chain. In addition, employees involved in hardware sourcing receive periodic training to maintain and enhance their knowledge of applicable global regulations and best practices. This may include, but is not limited to, attending webinars, roundtables, and conferences, or reviewing internal and external training materials.

Due diligence processes and remediation

Docusign Envelope ID: A8E0F3D7-F122-8DFE-83B3-625428BADFA2

Palo Alto Networks takes a risk-based approach to due diligence, focusing resources on sector and geographic specific risks, utilizing due diligence and continuous risk monitoring tools to help identify red flags relating to vendors and suppliers, and any failures to abide by their modern slavery obligations. In addition, we require selected direct suppliers, prioritized based on our risk assessment, to complete an annual questionnaire and to disclose certain labour practices and policies.

Palo Alto Networks maintains a culture of open communication and encourages anyone with a good-faith concern to speak up without fear of retaliation. We have implemented multiple internal and external communication channels to make it convenient for employees, business partners, and members of our community to ask questions, provide feedback, or report concerns. As outlined above, we require the same from our suppliers. Palo Alto Networks is committed to investigating any credible report of potential modern slavery or other applicable Code of Conduct violations in a fair, consistent, comprehensive, and objective manner. In line with our core beliefs, we confirm that we will take all appropriate and necessary steps to rectify any confirmed incidences of modern slavery in our operations or supply chains.

Assessing the effectiveness of actions taken to address modern slavery risks

During this reporting period, Palo Alto Networks assessed the effectiveness of our actions through the information collected in its annual partner surveys, conversations with suppliers, and the tools we utilized to conduct due diligence and assess risk.

Consultation

Palo Alto Networks is a well-integrated business. The same practices and procedures regarding responsible business and core ethics and compliance requirements apply to all subsidiaries, affiliates, and related entities around the globe. We have communicated with Palo Alto Networks (Australia) Pty Ltd and its subsidiary Sinefa Pty Ltd regarding this statement and our combined approach to modern slavery, mandating compliance with the policies and processes set out in this statement.

Approval

This Human Trafficking & Anti-Slavery Statement was approved by the Board of Directors of Palo Alto Networks (Australia) Pty Ltd on November 4, 2026.

DocuSigned by:
Stephan Engelmann
AF930FB6841D4C0...

Signed for and on behalf of Palo Alto Networks (Australia) Pty Ltd

Stephan Engelmann

Director, Palo Alto Networks (Australia) Pty Ltd

Docusign Envelope ID: 4E32F19A-CA4F-8A52-8108-3B7D93D1B1B6

MODERN SLAVERY STATEMENT FOR FINANCIAL YEAR 2025

This statement fulfills the requirements of Section 54 of the Modern Slavery Act 2015 and covers the period 1 January 2025 to 31 December 2025 for Cyber-Ark Software (UK) Limited.

Our Commitment

Being a sustainable leader in cybersecurity is as much about delivering the best services and solutions as it is about our people and our values that determine how we do business. We are committed to doing business with integrity, including protecting and advancing human dignity and human rights in our global business practices and throughout our supply chains, which is reflective of the UN Declaration on Human Rights.

CyberArk[1] does not tolerate or condone human trafficking, modern slavery, labor exploitation or any other human rights abuses in any part of our global organization. In any instance where such abuses are suspected, we will act swiftly to investigate and remedy the situation.

Who We Are

CyberArk, a Palo Alto Networks company, is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere.

Our Due Diligence Processes

All business partners and critical vendors are subject to automated due diligence screening at onboarding and throughout their lifecycle. This screening is facilitated via our integrated NAVEX platform, which explicitly evaluates third-party risk profiles for human rights and modern slavery vulnerabilities. Streamlined and centralized within our internal tracking databases, this framework routes elevated risk triggers to our Compliance team for in-depth evaluation.

As our corporate integration continues, these risk assessment mechanisms and screening protocols are being systematically aligned with Palo Alto Networks' global third-party risk management architecture.

Our Risk Assessment and Management

In general, CyberArk's human trafficking and modern slavery risks are relatively low. This is because our core business areas –the development, sale and support of software and cloud-based cybersecurity solutions – do not rely on low-wage labor or target vulnerable populations such as children or immigrants. We do not engage in any manufacturing or construction activities.

Additionally, CyberArk's vendors primarily include reputable technology vendors, technology service providers, professional service providers, and similar entities. At our offices, we purchase goods and services such as food, cleaning supplies, and marketing products from well-established local businesses. Similarly, our primary business partners are well-established distributors, resellers and technology partners, who typically do not rely on vulnerable populations or engage in manufacturing activities where human trafficking and modern slavery are most likely to occur.

[1] CyberArk Software Ltd. together with its global subsidiaries including Cyber-Ark Software (UK) Limited (CyberArk's United Kingdom incorporated trading entity for sales activities within the EMEA region), are referred to collectively in this statement as "CyberArk."

Docusign Envelope ID: 4E32F19A-CA4F-8A52-8108-3B7D93D1B1B6

Nevertheless, we recognize that human rights abuses can occur within any organization and its supply chain. With that in mind, we have worked to implement stronger policies and controls across our business and operations and supply chain.

Our Key Controls

We have continued maintaining controls across our business, including the following:

- **Strong Tone from the Top**: A demonstrated commitment from our Board and Management on conducting business with integrity.
- **Training and Awareness Programs**: We are continuously enhancing our training initiatives to ensure they are practical, cohesive, and tailored to meet organizational needs. These efforts focus on streamlining requirements and aligning training with compliance and operational objectives, thereby improving effectiveness and accessibility.
- **Code of Conduct:** Our Code of Conduct is designed to align with our values and practically address the compliance risks most relevant to our operations. It serves as the foundation for managing compliance and ethics risks at CyberArk, guiding our actions and supporting sound decision making, even in challenging situations.
- **Policies**: Our policies unequivocally denounce human trafficking and modern slavery and set forth a commitment to combatting such abuses. Our policies are reviewed annually.
- **Program Management**:
  - Our Compliance team is tasked with managing, overseeing and optimizing the in-house compliance program
  - Our Internal Audit team provides third line of defense audit support
  - Our global procurement function oversees procurement activities across our business operations and vets vendors in the supply chain
- **Reporting Channels**: Our publicly available reporting hotline allows for anonymous reporting of any suspected wrongdoing. We have raised awareness of our existing reporting channels during company-wide all-hands sessions and targeted training for high-risk teams and regions, including our confidential Speak Up hotline, which migrated to **Palo Alto Networks' Ethics Hotline** post acquisition. The Ethics Hotline remains available to our employees, business partners and other third parties.
- **Due Diligence Program:** We are screening our business partners and vendors at onboarding and throughout our engagement to enhance compliance with legal obligations and ethical values, monitoring for risks related to modern slavery or unethical labor practices.
- **Contractual Controls & Consequences:**
  - A contractual commitment by our business partners to comply with our Vendor and Business Partner Code of Conduct, or for legacy agreements, a requirement to respect applicable laws
  - Potential termination of the business relationship for a violation of the Vendor and Business Partner Code of Conduct

Our Key Performance Indicators

We are committed to continuous improvement in our ethics and compliance program, including measures to prevent modern slavery and other human rights abuses. Given our low risk profile, our primary key performance indicators (KPIs) relate to the number of incidents and reports to our Speak Up hotline, of which none were related to human rights or modern slavery in 2025. We also conduct annual employee

Docusign Envelope ID: 4E32F19A-CA4F-8A52-8108-3B7D93D1B1B6

certifications of our Code of Conduct and track compliance training completion rates. We will continue to monitor whether it is appropriate to add additional KPIs to increase the robustness of our control effectiveness assessments.

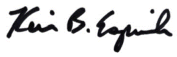
Our Training

To embed our core values into our daily operations, CyberArk delivers mandatory training programs covering our Code of Conduct, anti-corruption, data privacy, and cybersecurity. Throughout 2025, employees engaged with these compliance modules during mandatory new joiner inductions and via ongoing e-learning channels. Our Speak Up training continues to provide practical guidance on raising concerns safely and confidently. Moving forward, CyberArk's training program is being integrated and absorbed into Palo Alto Networks' centralized global compliance framework, ensuring a unified, platform-wide approach to human rights and ethical labor practices across all joint operations.

Approval

This Modern Slavery Act Statement was approved by the Board of Directors of Cyber-Ark Software (UK) Limited on November 4, 2026.

Signed by:



5052DCC647BE44C...