ISRAEL
Inspired by *innovation*

ISRAEL EXPORT INSTITUTE

Ministry of Economy and Industry
Foreign Trade Administration

Cyber Roadshow, Japan
March 2025

ISRAEL EXPORT INSTITUTE

Inspired by Innovation, Connected and Coordinated.

The Israel Export Institute, in cooperation with the trade mission to Japan and the Foreign trade administration at the Ministry of Economy, advances business relationships between Israeli exporters and overseas businesses and organizations.

By providing a wide range of export-oriented services to Israeli companies and complementary services to the international business community, the Institute helps build successful joint ventures, strategic alliances, and trade partnerships.

The Israel Export Institute (IEI) represents **over 500** exporting companies in the Cyber Security sector. Israeli Cyber companies offer technologically advanced, field-proven products and solutions that are among the most innovative anywhere. They are successfully partnering with key world players to ensure public safety, protecting Critical Infrastructure, Financial Institutions, Small and Big enterprises, Ports, Hospitals, Retailers, and more. The sector cooperates with Public and Governmental bodies and their agencies and with the private sector, promoting private industry joint ventures and international partnerships.

Discover Israel's Cyber Security Industry with IEI.

Miss. Ophri Hadar

Head of Cyber Unit
Tel: +972 52 8912 777
E-mail: ophrih@export.gov.il

Mr. Dan Shiff
Cyber Unit Business Development
Tel: +972 54 4329 400

E-mail: dans@export.gov.il

www.export.gov.il

駐日イスラエル大使館 経済部
Israel Economic & Trade Mission in Japan

ECONOMIC & TRADE MISSION IN JAPAN, EMBASSY OF ISRAEL

Based in Tokyo and Osaka, Israel’s Economic and Trade Mission in Japan creates exposure and business opportunities for Israeli companies in Japan, promotes inward investment, scouts for Israeli technologies for Japanese corporations and assist Japanese and Israeli companies to build partnerships. Reporting to the Foreign Trade Administration at the Ministry of Economy and Industry, our team collaborates with numerous partners in Israel and in Japan, to create a favorable business environment and foster bilateral relations in matters related to trade, investment, innovation and trade policy.

駐日イスラエル大使館経済部は、 東京と大阪を拠点に、 日本におけるイスラエル企業のプロモーションとビジネス機会の創出、対内投資の　促進、 日本企業のためのイスラエル技術の調査 ・ 発掘、 日本企業とイスラエル企業のパートナーシップ構築の支援などを行っています。　　イスラエル経済産業省外国貿易局の統括の下、弊部は、イスラエルと日本の数多くのパートナーと協力し、貿易 ・ 投資 ・ 技術革新・　貿易政策に関連する事項において、良好なビジネス環境を作り出し、二国間関係を促進しています。

Daniel Kolbar ダニエル・コルバー | Minister 経済公使
Head of Economic & Trade Mission 経済貿易ミッション代表
Embassy of Israel in Japan 駐日イスラエル大使館
T: +81-3-3264-0398 • Daniel.Kolbar@israeltrade.gov.il
Web (Japanese): www.israel-keizai.org

Kenji Ayao 綾尾 健嗣 | Trade Officer 商務官
Economic & Trade Mission to Japan
Embassy of Israel in Japan イスラエル大使館経済部
T: +81-3-3264-0398 • kenji.ayao@israeltrade.gov.il

Content

ActiveFence

ActiveFence protects online platforms, LLMs and governments from unwanted content.
https://www.activefence.com/

Categories

- Security Operations and Orchestration
- LLM
- AI
- Content safety
- Trust & Safety

Profile

ActiveFence provides AI-powered tools to help digital platforms, LLMs and governments protect users from online threats. Using advanced machine learning and threat intelligence, ActiveFence detects and mitigates a wide range of harmful content. **Key offering**: ActiveOS: a platform for orchestrating and operationalizing policy detection and enforcement. ActiveScore: AI-driven API that provides abuse-specific risk scores. GenAI Safety Solutions: comprehensive suite of GenAI Content Safety solutions covering a wide range of violations. Currently working with 7 of the top 10 LLMs, assisting in safeguarding both prompts and outputs layers. Threat intelligence: wide-ranging threat intelligence solutions designed to proactively identify and mitigate online threats before they manifest in the real world. Monitoring millions of online sources across open, deep and dark web, providing unparalleled visibility and insights to support complex investigations for enterprises and governments.The company protects billions of users across over 100 languages.ActiveFence is backed by investors in Silicon Valley and Israel, has raised $100M, and employs over 250 people worldwide.

Adversa

AI Red Teaming Platform - Security and Safety testing platform for AI and GenAI applications

https://adversa.ai

Categories

- Application and Website Security
- LLM
- AI
- AI Security

Profile

In Adversa AI, we are building a Security and Safety testing platform for GenAI applications - AI Red Teaming Platform. Adversa AI is Gartner-recognized leader in automated AI Red Teaming with customers in the US,EU and Asia.

Adversa AI Red Teaming platform is a groundbreaking end-to-end security solution tailored for AI applications, providing a level of security that traditional tools cannot match. Beyond simple vulnerability detection, we integrate comprehensive attack simulation, threat intelligence gathering, and continuous defense. This approach enables organizations to not only identify vulnerabilities in AI and GenAI applications but also understand, quantify, and preemptively mitigate exact risks within their AI systems.

Arnica

Arnica surfaces the right AppSec risk to the right owner at the right time with pipelineless, developer-native workflows.

https://www.arnica.io/

Categories

- Application and Website Security

Profile

Arnica's behavior-based platform for application security posture provides users with the first comprehensive pipelineless security approach which, in real-time, identifies and prevents software supply chain risk.

Our platform commoditizes full risk visibility, prioritization and ownership classification in a ‘free forever’ package for our customers. However; our growth, stickiness and momentum stem from a few key differentiators: Code changes are scanned ‘on push’ and provide a blameless and shameless feedback directly to developers via ChatOps.

Pull request merges can be enforced to prevent new high severity vulnerabilities and allows dev teams to mitigate the risks within a given SLA.

Automatic classification of the business importance of each code repository and the people that are best equipped to resolve issues within each repository. Validation of each hardcoded secret in the code repositories.

Cyberint a Check Point Company

Reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact.

https://cyberint.com/

Categories

- External risk protection
- Threat Intelligence

Profile

Cyberint, a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

Return to Contents

Hudson Rock

Cybercrime and Infostealer Intelligence Solutions.

https://www.hudsonrock.com/

Categories

- Network Security
- Anti-Fraud
- Authentication and IAM
- Security Operations and Orchestration
- Threat Intelligence

Profile

Cybercrime intelligence company that specializes in sourcing compromised credentials from Infostealer infections sourced directly from the threat actors.

Return to Contents

LayerX Security

The Enterprise Browser Extension.

https://layerxsecurity.com/

Categories

- Application and Website Security
- Network Security
- Data Protection Encryption and Privacy
- LLM
- AI

Profile

LayerX agentless Browser Security platform (delivered as an Enterprise Browser Extension) natively integrates with any browser, turning it into the most secure and manageable workspace, with no impact on the user experience. LayerX is the first solution that provides continuous monitoring, risk analysis, and real-time enforcement on any event and user activity in the browsing session

.Enterprises leverage these capabilities to secure their devices, identities, data, and SaaS apps from web-borne threats and browsing risks that endpoint and network solutions can't protect against. These include data leakage over the web, SaaS apps and GenAI tools, credential theft over phishing, account takeovers, discovery and disablement of malicious browser extensions, Shadow SaaS, and more.

Prompt Security

The Complete Platfo

https://www.prompt.security/

Categories

- Application and Website Security
- LLM
- AI

Profile

Prompt Security delivers a complete platform for securing Generative AI in enterprises. We empower organizations to safely adopt Generative AI while protecting them from the full range of risks. Our comprehensive solution addresses several key use cases.

Our solution for employees prevents shadow AI with real-time detection of AI sites used across the organization. It ensures data privacy when employees use tools like ChatGPT, Gemini, DeepSeek, Microsoft Copilot, or GitHub Copilot, among many others, by sanitizing sensitive data before it reaches the LLM behind these tools. Prompt Security also provides a security and content moderation solution for homegrown AI applications, protecting from risks like prompt injection attacks, content toxicity, and data leakage.

The platform enables enterprises to fully embrace Generative AI with confidence while maintaining complete visibility and control over their AI interactions.

Return to Contents

RubyComm

Dedicated OT Cybersecurity for Manufacturers and Infrastructure.

https://www.rubycomm.com/

Categories

- OT and Industrial Control System
- Medical IoT
- Cybersecurity for manufacturing and critical infrastructure

Profile

RubyComm is a developer and manufacturer of easy-to-install cybersecurity appliances specialized to protect OT (Operational Technology) equipment and sensitive corporate communications. Our flagship product, Rubyk™ OT, is a line of compact, affordable security appliances tailored to provide customizable cybersecurity protection to connected assets across a wide variety of industry segments. Our solution is unique in the fact that it does not require network experts to install, and can be used with both new and aging legacy devices.

Sasa Software

Sasa Software specializes in cybersecurity, focusing on preventing file-based attacks.

https://www.sasa-software.com/

Categories

- Application and Website Security
- Network Security
- End Point Security
- OT and Industrial Control System

Profile

Sasa Software's GateScanner line uses **Content Disarm and Reconstruction (CDR)** technology to effectively block both known and previously undetected threats, including malware, viruses, ransomware, zero-day attacks, and other targeted threats. Trusted by top-tier government agencies in the **APAC region**, including Japan and Singapore, **Sasa Software** offers robust network protection for critical infrastructure, financial institutions, and a wide range of industries. We're working with sectors like global energy, water, law offices, banks, insurance companies, and healthcare.

As we look to expand in Japan, we are seeking to collaborate with local partners, including system integrators and **Managed Security Service Providers (MSSPs)**, to deliver our advanced **CDR** solutions to customers looking to enhance their defenses against file-based attacks. **Sasa's** solutions provide comprehensive protection across all data routes, including **email**, **API's**, **USB devices**, and **secure managed file transfers**. Our technology integrates seamlessly into existing workflows, enhancing overall security while eliminating file-based threats.

Come and meet us to explore potential collaboration opportunities and discuss how we can work together to improve cybersecurity for Japanese organizations.

Silverfort

Silverfort secures every dimension of identity.

https://www.silverfort.com/

Categories

- Anti-Fraud
- Authentication and IAM
- OT and Industrial Control System
- IoT
- Medical IoT

Profile

Silverfort provides a Unified Identity Protection platform that secures access to all sensitive assets across hybrid and multi-cloud environments. By extending identity-based security controls, Silverfort protects systems that were previously unprotected due to technological or operational limitations, such as homegrown applications, legacy systems, command-line interfaces, and more. It enables real-time risk assessment and enforces adaptive access policies without requiring agents or inline proxies, offering seamless integration with existing identity infrastructure. Silverfort's unique approach eliminates blind spots in identity security, helping organizations prevent threats like ransomware, lateral movement, and privilege escalation.

With its centralized visibility and policy enforcement, Silverfort simplifies compliance with identity-centric regulations and provides enhanced security for modern and legacy systems alike. Trusted by enterprises worldwide, Silverfort ensures robust identity protection while maintaining a frictionless user experience.

Sling Insurtech LTD

Automated, real-time cyber risk monitoring and scoring.
https://www.slingscore.com/

Categories

- Cyber Risk Assessment

Profile

Sling delivers a third-party cyber risk assessment solution powered by extensive monitoring capabilities. With its advanced, in-house assessment technology, Sling enables companies to evaluate their supply chain security posture in real time, ensuring risk is measured accurately and consistently.

The platform combines advanced Cyber Threat Intelligence (CTI), drawing insights from the Dark Net, Deep Web, and Technical Intelligence with comprehensive Attack Surface Monitoring (ASM). This integration provides a predictive risk score that assesses a company's likelihood of being targeted by a cyberattack.

Sling offers an extensive view of emerging threats, helping companies identify high-risk vendors and proactively prioritize and address vulnerabilities.

Return to Contents

Sygnia

Beat Attackers. Stay Secure.

https://www.sygnia.co/

Categories

- Application and Website Security
- Cloud and Infrastructure Security
- Network Security
- Data Protection Encryption and Privacy
- End Point Security
- OT and Industrial Control System
- IoT
- Security Operations and Orchestration

Profile

Sygnia is the foremost global cyber readiness and response team, applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. With a team of deep digital combat and enterprise security specialists, Sygnia enables companies to proactively build cyber resilience and defeat attacks within their networks. At each phase of the security journey, Sygnia delivers the tailored insight, technological acumen and decisive action needed for their clients to be unstoppable in the face of cyber threats. Sygnia is a trusted advisor and service provider of technology and security teams, executives and boards of leading organizations worldwide, including Fortune 100 companies. Sygnia is a Temasek company and part of the ISTARI Collective.

Transmit Security

Transmit Security delivers a fusion of identity management, verification, and fraud prevention.

https://transmitsecurity.com/

Categories

- Application and Website Security
- Mobile Security
- Anti-Fraud
- Authentication and IAM

Profile

Transmit Security, the leading innovator of fraud prevention and identity security, has developed the industry’s only platform with a fusion of natively-built customer identity management, identity verification and fraud prevention services in one platform. Mosaic by Transmit Security provides best-of-breed modular services, including orchestration and a complete set of authentication methods — from passkeys to passwords. Addressing complicated fraud and identity use cases, it optimizes security and CX while minimizing costs and complexity. With AI-driven cybersecurity in its core, Mosaic is built for resiliency and scale, earning the trust of 7 ‘top 10’ US banks and Fortune 500s.

Waterfall Security Solutions

Enabling critical OT operations with hardware-enforced protection.

https://waterfall-security.com/

Categories

- Cloud and Infrastructure Security
- Data Protection Encryption and Privacy
- OT and Industrial Control System
- Security Operations and Orchestration

Profile

Enabling critical OT operations with hardware-enforced protection. Waterfall Security makes hardware-enforced cybersecurity products that are used for protecting the OT networks of critical infrastructures around the world. For nearly 20 years, sensitive industries and critical infrastructures have trusted Waterfall to guarantee safe, secure, and reliable operations. Waterfall's global install-base includes power plants, nuclear reactors, onshore/offshore oil & gas facilities, refineries, manufacturing plants, water utilities, railways, airports, casinos, data centers, governments, defense companies, and mining operations. Waterfall's patented technologies leverage the benefits of combining hardware with software to deliver Engineering-grade security that enables industrial operations to continue running in the ever-evolving OT threat environment.

This publication is for informational purposes only. While every effort has been made to ensure the information is correct, The Israel Export & International Cooperation Institute assumes no responsibility for damages, financial or otherwise, caused by the information herein.