ISRAEL

ISRAEL EXPORT INSTITUTE

Ministry of Economy and Industry
Foreign Trade Administration

NTT
Innovation Laboratory Israel

THE ISRAELI EVENT
AT RSA

April 28, 2025 | SAN FRANCISCO
10 AM-3 PM

B2B WILL BE OPEN UNTIL 5 PM

ISRAEL'S CYBER SOIRÉE AT RSA »

ISRAEL EXPORT INSTITUTE

THE ISRAEL EXPORT & COOPERATION INSTITUTE

The Israel Export & International Cooperation Institute, a nonprofit organization supported by the government of Israel and the private sector, facilitates business ties, joint ventures and strategic alliances between overseas and Israeli companies. Charged with promoting Israel's business community in foreign markets it provides comprehensive, professional trade Information, advice, contacts and promotional activities to Israeli companies. Furthermore, the IEICI provides complementary services to business people, commercial groups, and business delegations from across the globe: IEICI uses its unique and one of a kind network with the prosperous startup ecosystem in Israel, and connects the foreign players, according to their field of interest.

Ophri Hadar • Head of Cyber and Fintech Sectors
• Ophrih@export.gov.il • T: +972 (52) 8912777

Ministry of Economy and Industry
Foreign Trade Administration

THE FOREIGN TRADE ADMINISTRATION AT THE ISRAELI MINISTRY OF ECONOMY & INDUSTRY

The Foreign Trade Administration is an agency within the Israeli Ministry of Economy and Industry responsible for promoting and facilitating Israel's international trade activities.

Its main objective is to expand Israel's exports, attract foreign investments, and strengthen economic ties with other countries.

The Foreign Trade Administration operates through more than 50 Economic and Trade Missions worldwide, assisting Israeli businesses in accessing foreign markets and identifying potential partners and opportunities.

- **Mr. Nathan Tsror** • Director, Americas Department
- nathan.tsror@economy.gov.il

- **Mr. Asaf Argov** • Project Manager
- asaf.argov@economy.gov.il

- **Mr. Shai Pascal** • Project Manager
- shai.pascal@economy.gov.il

Israel Economic Mission
West Coast of the USA

THE ISRAEL ECONOMIC AND TRADE MISSION TO THE WEST COAST

The Israel Economic and Trade Mission to the West Coast is the official representation of Israel's economic interests in the western region of the United States.

It serves as a liaison between Israeli businesses and potential corporates and investors on the West Coast.

The Mission focuses on promoting trade and investment opportunities, fostering innovation and technology collaborations, and strengthening economic ties between Israel and 17 states on the West Coast states, such as California, Washington, Oregon, and Minnesota.

Through various events, conferences, and networking opportunities, the Mission aims to facilitate bilateral economic growth and cooperation in key sectors like technology and AI, cybersecurity, fintech, healthcare, retail tech, agtech, and more.

• **Mr. Omer Fein** • Chief Economic Consul
• omer.fein@israeltrade.gov.il • C: (415) 518-3909 •

• **Mr. David Bedrosian** • Business Development Manager, Cybersecurity
• david.bedrosian@israeltrade.gov.il • C: (650) 995-1457

NTT Innovation Laboratory Israel

NTT Innovation Laboratory Israel NTT (Israel) is a first-of-its kind focal point to NTT group in Israel. NTT is a 150-year-old global corporate (HQ Tokyo), a world leader in providing technology and business solutions to people, clients, and communities. With almost $100B in annual revenue, NTT has more than 900 subsidiaries and is a Fortune 100 company.

NTT Israel creates collaborations between the Israeli innovation ecosystem and the NTT group and its customers by focusing on three main activities:

Initiating and facilitating commercial transactions between Israeli tech companies and the NTT group and customers

Promotion of investments by the NTT group

Co development with Israeli companies and academia to generate new services.

• **Moshe Karako** • CTO
• Moshe.karako@global.ntt
• nttinnovation.labisrael@global.ntt
• global.ntt/NTT-Israel.html

CONTENT

Bullet proofing your IAM against cyber attack and human errors

Uninterrupted Access in an Increasingly vulnerable SaaS threat landscape. Acsense reduces IAM downtime to ensure greater visibility and uninterrupted access to enterprise SaaS applications. Acsense also proactively mitigates risk with its disaster recovery solution tailored to the specific needs of IAM (IAM Ransom). Acsense customers enjoy peace of mind while strengthening compliance, staying audit-ready, and meeting stringent regulatory requirements.

CATEGORIES:

- Application and Website Security
- Cloud and Infrastructure Security
- Anti-Fraud, Authentication and IAM

ADVERSA

www.adversa.ai

Continuous Security Platform for custom GenAI applications and agents.

Adversa is the world's first and only risk-focused Continuous Red Teaming platform for GenAI, born from groundbreaking AI research and recognized by industry leaders like Gartner and IDC. From day one, we've set the standard for AI security, earning the trust of Fortune 500 companies, AI Decacorns, and the Big 4 across the US, EU, Middle East, and Asia.

The platform conducts red teaming of AI applications and agents, not only detecting vulnerabilities but also prioritizing them based on business risks unique to each application while facilitating remediation.

This process is performed continuously, delivering a level of security that is impossible to achieve with standalone guardrails or firewalls. Adversa enables enterprise AI transformation by providing security and safety infrastructure, as well as ensuring compliance with regulations for the development and use of AI apps, even in critical business processes and highly regulated environments.

Adversa AI isn't just protecting the future of AI—we're defining it.

CATEGORIES:

- Application and Website Security
- Cloud and Infrastructure Security
- Anti-Fraud
- Authentication and IAM

Modern AppSec via Reachability Analysis Breaking the Boundaries of Traditional SAST and SCA Security Scanners.

At Backslash Security, we do AppSec differently—so you can focus on what matters. Our App Graph model redefines how code is understood and secured. Using Reachability Analysis, we go beyond traditional SAST and SCA tools to help you prioritize real risks and secure your applications smarter and faster.

CATEGORIES:

- Application and Website Security
- AppSec
- Product Security
- Code Security

Know your data. Control your data

BigID is a leader in data security, privacy, compliance, and governance: enabling organizations to proactively discover, manage, protect, and get more value from their data in a single platform for data visibility and control. Customers use BigID to reduce their data risk, automate security and privacy controls, achieve compliance, and understand their data across their entire data landscape: including multicloud, hybrid cloud, IaaS, PaaS, SaaS, and on-prem data sources.

BigID has been recognized by CNBC as one of the top 25 startups for the enterprise, has been named to the Inc 5000 and Deloitte 500 for two years in a row, and is the leading modern data security vendor in the market today.

CATEGORIES:

- Cloud and Infrastructure Security
- Data Protection Encryption and Privacy
- GRC and Vulnerability Management
- Data security posture management (DSPM)
- Datasecurity privacy
- ai governance

Breeze builds cyber resilience and vigilance for organizations by adaptively strengthening defenses against business-critical threats.

Breeze solution contextualizes organisations' exposures and gaps with an up to date threat modeling to safeguard critical assets and key accounts against relevant threat actors TTPs by remobilizing and optimizing defenses, allowing preemptive remediation and predictive vigilance.

CATEGORIES:

- Cloud and Infrastructure Security
- GRC and Vulnerability Management
- Security Operations and Orchestration
- LLM
- AI
- CTEM
- ASCA
- Cyber Resilience & Cyber Vigilance

Misinformation Threat Management

Brinker is an end-to-end misinformation threat management platform that serves the public sector and major enterprises. It combats online harassment, from malicious narratives to impersonation, using proprietary content analysis, AI-enabled detection, and automated OSINT investigations. The platform offers a suite of mitigation tools at the press of a button, including pre-legal action, media publication, content removal, and counter-narratives

CATEGORIES:

- LLM
- AI
- Disinformation, misinformation
- influence
- Cyfluence
- malicious narratives
- Threat intelligence

Readiness and Resilience Through Tech-Driven Education

CyberproAI's Three Strategic Vectors: Education / Technology / CyberOps Defense. At CyberproAI we combine military-grade playbooks with real-world cyber operations to create future-ready solutions and train talent in cyber defense & AI, powered by advanced technologies and education.
Training the Next Generation of Cyber and AI Leadership. We take pride in being at the forefront of cyber defense. With decades of proven experience, our team provides continuous training to our global clients while working closely with them. This collaborative approach gives us a unique advantage in identifying and nurturing raw talent, teaching fundamentals, and training elite professionals in cutting-edge techniques while simultaneously committing to the adaptation and development of advanced military-grade technologies that meet the evolving needs of the cyber domain, ensuring optimal protection at every level.

The Human Factor is Key
At CyberproAI we believe that technology is a story that revolves around people, not just products. With global talent and local understanding, we build ecosystems that foster collaboration and promote rapid growth.

CATEGORIES:

- cyber education
- cyber training
- AI

Cybord

www.cybord.ai

Inspect. Trace. Secure. AI-powered component integrity and traceability

Cybord is revolutionizing how companies relying on discrete electronics ensure product security and reliability through advanced visual AI inspection and traceability. Addressing growing concerns over supply chain security, component authenticity, and material origin, we offer unmatched protection against cyber-physical threats. Our software analyzes 100% of components during assembly, detecting counterfeit parts, unauthorized substitutions, and tampering in real time. By ensuring every component meets security and compliance standards, Cybord safeguards critical systems in defense, aerospace, automotive, and data centers from supply chain vulnerabilities.

CATEGORIES:

- Automotive Security
- AI

CYFOX: AI-driven cybersecurity bridging gaps for MSSPs & SMEs

CyFox's all-in-one XDR platform is tailored for Managed Security Service Providers (MSSPs) and Small-to-Medium Enterprises (SMEs).
Powered by advanced AI, it streamlines threat detection, reduces tool sprawl, simplifies integrations, and minimizes operational costs—delivering unmatched efficiency, scalability, and protection.Introducing CYFOX OmniSec, our next-generation virtual CISO (vCISO) solution designed to combat modern cyber threats and simplify compliance.
Complementing these is MailSecure, our cutting-edge email security solution, engineered to block advanced phishing attacks, malware, and data leaks.Together, CyFox's suite of tools empowers MSSPs and SMEs to enhance service delivery, strengthen defenses, and optimize operations in today's complex cyber landscape

CATEGORIES:

- Cloud and Infrastructure Security
- Network Security
- Data Protection Encryption and Privacy
- End Point Security, IoT
- Medical IoT
- Automotive Security
- Security Operations and Orchestration
- LLM
- AI

CYBER CRISIS READINESS AND MANAGEMENT PLATFORM

Founded by seasoned crisis managers with extensive experience handling international cyber crises, Cytactic's SaaS platform provides a comprehensive solution for cyber crisis readiness and management. Cytactic's platform is designed to bring order to the chaos of cyber crises. It equips organizations with advanced simulations, readiness programs, and tools to address human, technical, and regulatory challenges and serves as the backbone of every business, helping them prepare for and manage crises while reducing overall impact and uncertainty. During a cyber crisis, when every minute and every decision counts, the Cytactic platform ensures that all relevant roles are trained, prepared, and coordinated to manage cyber crises or incidents in a structured, orchestrated manner, making real-time adjustments as needed.

CATEGORIES:

- GRC and Vulnerability Management
- Security Operations and Orchestration

Protecting Every Message, Call, and Connection

Cyvore provides Centralized Workspace Security which offers a comprehensive view and insights.
Cyvore zeroes in on the full spectrum of digital environments where human interaction takes place, from Zoom, Teams and Email to Slack, WhatsApp, CRM and beyond, ensuring protection against any potential attack surface, like never seen before.

CATEGORIES:

- End Point Security
- Centralized Workspace Security

Deepkeep provides AI native security and trustworthiness for AI\ LLM

DeepKeep empowers large the alignment is both sides, while the rest is left-sided. please make it the same as the other companies. error-free, secure, and trustworthy AI solutions. This includes vision data models, LLMs and multimodal in risk assessments, prevention, detection, monitoring, and mitigation.

CATEGORIES:

- Cloud and Infrastructure Security
- Automotive Security
- LLM
- AI Security
- governance
- adversarial attacks.

AI Powered Asset Intelligence Platform

DeviceTotal is a leading cybersecurity company offering an agentless platform for proactive risk assessment and management of IoT, OT, and network-connected devices. Headquartered in Singapore, DeviceTotal enables organizations to identify, prioritize, and mitigate security risks across their device ecosystems. The platform provides an accurate risk score for each device, along with detailed insights on vulnerabilities, end-of-life (EOL) status, and actionable mitigation and remediation data.

These insights allow organizations to prioritize actions effectively, ensuring efficient risk management and security optimization. With data updated daily, DeviceTotal delivers ongoing visibility into device security postures, helping organizations stay ahead of emerging threats while maintaining operational resilience. Trusted by global enterprises, DeviceTotal simplifies complex cybersecurity challenges with actionable intelligence and tailored recommendations. DeviceTotal's unique approach empowers businesses to manage device security comprehensively, making it an essential solution for safeguarding critical infrastructure and achieving long-term security goals.

CATEGORIES:

- Network security
- End point security
- OT & IOT
- Risk Management

Prevent the Undetetctable

Sasa Software specializes in proactive protection of networks from file based attacks utilizing Content Disarm and Reconstruction (CDR) file sanitization technology, to neutralize known and unknown malicious content in emails and files.
The company's award-winning GateScanner suite offers CDR content sanitization that is natively embedded into channel-specific applications. From a Secure Email Gateway, through a Secure Managed File Transfer solution, a safe USB Import Station (Kiosk) or an API/ICAP-based 'CDR as a Service' solution - GateScanner provides elevated data security on a broad range of network configurations and use cases.
Sasa Software's long-term clients include more than 450 organizations in government, financial services, critical infrastructure, oil gas & energy, shipping, pharmaceuticals, healthcare, pharmaceuticals and defense and more, across four continents.

CATEGORIES:

- Cloud & infrastructure security
- Network security
- Data protection & encryption
- Email security

Machine Unlearning Platform: Remove Unwanted Data & Behaviors from AI Models

Hirundo is the first Machine Unlearning solution in the world – making AI "forget". Despite solutions like data cleaning and guardrails, trained/finetuned AI models are still infested with problematic data and behaviors that put organizations at risk. Data that is confidential, malicious, poisoned or personal; and behaviors like biases, hallucinations, toxicity.Hirundo's platform allows to remove any unwanted data, knowledge or behaviors from LLMs, without lengthy retraining/finetuning. It doesn't just filter them, but actually removes these from the model itself, remediating the problems at depth.Hirundo's technology is protected by 5 filed US patents, co-developed by its Chief Scientist, previously the Dean of Computer Science and E-VP at the Technion.

CATEGORIES:

- Data Protection Encryption and Privacy
- LLM
- AI

Frictionless fraud prevention from sign- to sign-out across all your channels

IronVest is an emerging leader in financial fraud prevention, reimagining the way high-risk transactions are authenticated and protected. Our patented technology called AuthenticAction™ combines real-time live biometrics with user actions, to deliver a seamless user experience from sign-in to post sign-in while ensuring the integrity of digital interactions.
Designed for industries handling sensitive transactions, IronVest provides deterministic security signals that verify actions in real time, before any financial loss happens, unlike traditional statistical models prone to errors. This ensures robust protection against fraud while significantly reducing operational costs for organizations.
By empowering financial institutions with reliable, proactive account security solutions, IronVest is transforming digital trust and efficiency. Trusted by partners worldwide, we are committed to driving innovation, safeguarding users, and enabling seamless, secure online interactions.
IronVest is ushering in the future of digital banking. Zero fraud and zero friction.

CATEGORIES:

- Anti fraud
- Authentication
- GRC
- Real tine biometrics

ITsMine Managed Data Protection (MDP) platform, a proactive and agentless platform that protects data everywhere.

The ITsMine Managed Data Protection (MDP) platform is a proactive, agentless solution that safeguards data everywhere.

Main Use Cases:
1. **Ransomware Attacks:** In 2024, attacks like IOCP, REvil, and CLOP involve data leakage followed by encryption. ITsMine:
• Alerts in real time • Provides a full list of stolen files.• Kill critical files, even on external offline systems.

2. **Secure File Sharing Between Companies:** Robust security measures for inter-organizational file sharing include:
• File GPS: Protects files at rest, in motion, and in use, even beyond company boundaries • Call Home: Notifies the central control system whenever files are accessed • Centralized Control: Files have a metaphorical "time bomb," limiting their availability outside the virtual vault • Kill Files: Remotely deactivate files if necessary, even on external offline systems.

3. **AI Tools:** Utilizing AI tools like Microsoft Copilot and ChatGPT to scan files outside the ITsMine virtual vault.
These features create a robust shield around sensitive files, ensuring their safety both within and outside the organization.

CATEGORIES:

- Data Protection
- Encryption
- Privacy
- DLP
- DRM
- Encryption less
- Ransomware

KELA

www.kelacyber.com

External Threat Exposure Reduction- Proactive, continuous, intelligence-driven.

KELA's Unified Threat Intelligence Platform is an all-in-one solution for Cyber Threat Intelligence (CTI), External Attack Surface Management (EASM), Digital Risk Protection Services (DRPS), and Third-Party Risk Management (TPRM), delivering real-time, actionable insights. The platform protects identities, brands, digital exposure, and the supply chain, seamlessly integrating into existing security controls and acting as the first line of defense against cyber threats from the cybercriminal underground. It monitors national risks, critical infrastructure, and supports dark web and cybercrime investigations, helping organizations close security gaps and stay ahead of evolving threats. KELA serves hundreds of customers, including enterprises, MSSPs, law enforcement agencies, CERTs, and government agencies worldwide.

CATEGORIES:

- Threat intelligence
- Dark web monitoring
- EASM
- TPRM

Your organization is already using GenAI. Lasso to protects every interaction with LLMs—simple, seamless, secure.

Lasso Security is a GenAI security platform that enhances security posture by autonomously monitoring all GenAI interactions, detecting risks in real time, and enabling organizations to effortlessly safeguard their GenAI activities.

CATEGORIES:

- Application and Website Security
- Data Protection Encryption and Privacy
- LLM
- GenAI Security
- LLM Security
- LLM
- Data Protections
- Application Security
- Generative AI

The Enterprise Browser Extension

LayerX Security offers an all-in-one, agentless security platform that protects enterprises against the most critical risks and threats of the modern web, including GenAI data leakage, SaaS risk, identity threats, web vulnerabilities, DLP, and more. LayerX is deployed as an Enterprise browser extension that integrates with any browser and provides organizations with full last-mile visibility and enforcement without disrupting the user experience. Enterprises use LayerX to secure their hybrid workforce in a SaaS-first world.

CATEGORIES:

- Network Security
- Data Protection Encryption and Privacy
- AI
- Browser Security

www.mile.st

Milestone - Disrupting Cyber Consulting Services

Milestone - Disrupting Cyber Consulting Milestone is the smarter alternative to the Big 4, offering an AI-powered, SaaS-based cybersecurity consulting platform that redefines how enterprises engage with security services—just as Airbnb transformed the hotel industry. We deliver the best of both worlds: the trust and reliability of a large firm, combined with the agility and deep expertise of top specialists. With AI-driven efficiency and expert insights, Milestone makes cybersecurity consulting smart, fast, and efficient—all through a seamless, cutting-edge digital experience.

CATEGORIES:

- Application and Website Security & Mobile Security
- Cloud and Infrastructure Security & Network Security
- Anti-Fraud
- Authentication and IAM
- Data Protection Encryption and Privacy
- End Point Security
- OT and Industrial Control System
- IoT & Medical IoT
- Automotive Security
- GRC and Vulnerability Management, Security Operations and Orchestration
- LLM
- AI

Application Security for No-code, RPA, and GenAI

Nokod Security offers application security and governance for applications and automations developed in low-code / no-code (LCNC) and RPA environments such as Microsoft Power Apps, UiPath, ServiceNow, etc. The product detects vulnerabilities and compliance issues and allows for managing a governance policy in a field currently invisible to security teams and considered a Shadow Engineering area.

CATEGORIES:

- Application and Website Security
- Data Protection Encryption and Privacy
- AI
- Application Security for No-code
- RPA, and GenAI
- LCNC, robotic process automation
- Microsoft Power Platform
- UiPath
- Servicenow

Unified AI-Driven Remediation Platform

Opus Security is a cloud-native remediation platform revolutionizing vulnerability management. Designed for enterprise security teams, Opus consolidates and de-duplicates vulnerability data across tools, providing a unified view enriched with business-critical context. Our AI-driven Multi-Layer Prioritization Engine identifies high-risk vulnerabilities based on exploitability, asset criticality, and real-world threats, ensuring teams focus on what matters most.

Opus automates the end-to-end remediation lifecycle, from assigning issues to responsible developers to tracking progress and validating fixes. By integrating seamlessly with tools like Slack, Jira, and CI/CD pipelines, Opus eliminates manual processes and silos, enabling efficient cross-team collaboration.

Purpose-built for dynamic environments, Opus empowers organizations to reduce exposure, improve security hygiene, and meet compliance requirements with minimal effort. Trusted by forward-thinking companies, Opus is setting a new standard in vulnerability management, transforming operational chaos into clarity and driving measurable security outcomes.

CATEGORIES:

- Cloud and Infrastructure Security
- GRC and Vulnerability Managemet
- Security Operations and Orchestration
- Vulnerability Remediation

Securing the AI lifecycle

Pillar is a unified, end-to-end AI security platform that proactively identifies and mitigates risks across the full AI lifecycle—covering data, development, and production. By uniting AI fingerprinting, LLM asset inventory, and seamless integration with code repositories, cloud infrastructures, and ML data platforms, Pillar ensures full transparency and secure, compliant operations. Through proactive red-teaming and adaptive guardrails, Pillar hardens AI models against evolving threats. Aligned with leading industry frameworks and standards, it ensures compliance, transparency, and continuous protection for advanced AI agents.

CATEGORIES:

- LLM
- AI
- Ai discovery
- AI-SPM
- Red teaming, guardrails, monitoring and tacing

www.prompt.security

The Complete Platform for GenAI Security

Prompt Security delivers a complete platform for safeguarding every aspect of Generative AI in the organization. From preventing Shadow AI and data privacy risks associated with the use of GenAI tools and copilots by employees, to protecting from Prompt Injection, Jailbreaks, and other GenAI risks in homegrown applications..

CATEGORIES:

- Application and Website Security
- LLM
- AI Security
- GenAI Security
- AI Governance

RESCANA

www.rescana.com

Rescana is an autonomous Third-Party Risk Management (TPRM) platform that streamlines and automates the identification and mitigation of vendor cyber risks.

Rescana is an advanced autonomous Third-Party Risk Management (TPRM) platform designed to simplify and automate the process of identifying, assessing, and mitigating risks associated with third-party vendors. By leveraging cutting-edge AI technology, Rescana provides organizations with real-time insights into their vendor ecosystem, ensuring compliance, enhancing security, and reducing operational burdens. Its user-friendly interface and powerful automation capabilities make it an ideal solution for organizations aiming to streamline their risk management processes while maintaining a robust security posture.

CATEGORIES:

- GRC and Vulnerability Management
- TPRM Third Party Risk Management platform

www.resec.co

Zero Trust Ransomware Prevention at the Gateway

Resec is redefining gateway security by providing organizations with unparalleled protection from file-based malware threats without hindering business flows and usability.

Resec's Zero Trust Prevention platform combines advanced detection and prevention technologies to provide IT security complete control of what enters their organization, while eliminating all known and unknown ("zero day") malware threats from all common gateway threat vectors. Resec's innovative technology also prevents threats coming from AI-generated files and provides coverage for encrypted content, extra-large files, and unique file formats.

Resec is trusted by some of the world's most sensitive organizations, including major financial institutions, critical infrastructure, telcos, retail, government, insurance, and military and defense organizations.

CATEGORIES:

- Application and Website Security
- Network Security
- Email security
- CDR
- Zero trust

Rig

www.rig.security

Our goal is to equip enterprises with actionable insights to fix identity risks and meet compliance needs

Rig Security, founded by Guy Kozliner (Wiz, Special Forces) and Nissim Bitan (Aqua, Mamram), is tackling the $17 billion and rapidly growing identity protection market with a revolutionary platform that consolidates fragmented IAM and security data into a unified framework focused on access risk remediation using AI. With 80% of all breaches involving compromised identities, Rig equips enterprises with actionable insights to fix identity risks and meet compliance needs. Backed by top Cybersecurity VCs and industry leaders from Wiz and Crowdstrike, Rig's innovative approach and exceptional team position it to lead the identity protection space.

CATEGORIES:

- Anti-Fraud, Authentication and IAM
- AI
- Identity Security
- Identity Risk Management
- Identity Threat Detection
- SaaS Security
- Security Posture Management

Cyber Recovery Platform for ICS/OT

Salvador Technologies provides a cyber recovery platform for downtime prevention in Industrial Control Systems (ICS) and Operational Technology (OT) organizations. Its innovative solution minimizes downtime and regains operations immediately after a cyber-attack, IT outage, or NY Windows failure incident, in a record timeframe of 30 seconds.
The company's platform is used by some of the world's most secure critical infrastructure organizations, including manufacturing, aerospace, maritime, energy and water companies.

CATEGORIES:

- OT and Industrial Control System
- Automotive Security
- Security Operations and Orchestration
- SIEM

Scribe

www.scribesecurity.com

Software Supply Chain Security SaaS Platform

Scribe Security is a comprehensive software supply chain security platform designed to secure your software products, CI/CD pipelines, and SDLC processes from development to deployment, ensuring continuous integrity and compliance across the entire product lifecycle.
Scribe Security proactively secures software supply chains with policy guardrails, automated SBOM management, cryptographic attestations, and compliance enforcement—without slowing development or time to market. Unlike traditional AppSec tools that focus only on detecting vulnerabilities, Scribe ensures every artifact, pipeline and process is tamper-proof and compliant before deployment.

CATEGORIES:

- Application and Website Security, Cloud and Infrastructure Security,
- Software Supply Chain Security

See What You've Been Missing

Sepio provides the first trafficless CPS platform based on device existence. The company's solution offers customers actionable visibility, policy enforcement and mitigation capabilities, allowing them to manage their assets' risk. The solution does not require any traffic or activity monitoring – and as such is use case and device agnostic, whether it is IT/OT/IoT or IoMT. If an asset connects to your infrastructure, Sepio will report it. At any scale, within less than 24 hours, you can see, assess and mitigate your assets' risks, streamline your operations and strengthen your cybersecurity posture.

CATEGORIES:

- Network Security
- End Point Security
- OT and Industrial Control System
- IoT
- Medical IoT
- GRC and Vulnerability Management
- Mitigation

Unified Identity Protection (human and non-human)

Silverfort provides unified identity protection for enterprises by extending Multi-Factor Authentication (MFA) and Zero Trust security to any resource, including legacy systems, command-line interfaces, and on-prem environments, without requiring agents or proxies. Its platform leverages AI-driven risk analysis to prevent identity-based attacks such as lateral movement, ransomware, and credential compromise. Silverfort seamlessly integrates with existing identity providers like Microsoft Entra ID and Active Directory, enhancing security across cloud and hybrid environments. By enforcing adaptive authentication and continuous access policies, Silverfort ensures secure access to sensitive systems without disrupting workflows.

CATEGORIES:

- MFA
- NHI
- Non-human identities
- Service Accounts
- PAS
- PAM
- Expansion (active in 5 and more markets)

Enterprise Browser & Extension

SURF is a transformative enterprise browser that establishes seamless, secure, zero trust access from any device for any user, including 3rd parties, to deliver immediate productivity.
SURF can extends conditional access to privileged administrators and developers, enabling productivity from any device. SURF further renders top threats like Phishing and Ransomware irrelevant.

CATEGORIES:

- Application and Website Security
- Network Security
- Data Protection Encryption and Privacy
- AI
- zero trust
- DeepFake

SaaS Security

Suridata's SaaS runtime security solution detects and prevents breaches originating from SaaS applications, safeguarding enterprises against exploitation of existing attack paths.

The extensive use of SaaS applications, APIs, and service accounts creates a complex SaaS network with thousands of interconnections. Suridata maps this network and the associated risks, connects the dots to understand the attacker's perspective, and identifies active attack paths that can be exploited. With Suridata's solution, security teams can break these attack paths and respond to critical risks effectively.

CATEGORIES:

- SaaS
- Third-parties

SYGNIA

www.sygnia.co

It is a promise we take seriously. We fortify defenses. We contain threats and defeat attacks. We keep your business up and running.

Sygnia's holistic, end-to-end solution set spans proactive and reactive cyber security. From executive-level strategic guidance to on-the-ground technical expertise, our incident response-fueled services enable our clients to be cyber ready in times of crisis and calm.

CATEGORIES:

- Cloud and Infrastructure Security
- Network Security
- Anti-Fraud
- Authentication and IAM
- OT and Industrial Control System
- MDR

TerraZone

TerraZone: Unified cybersecurity platform with ZTNA, microsegmentation, and endpoint protection

TerraZone is a cybersecurity innovator offering a patent-based Zero Trust Unified Security Platform that addresses the challenges of modern digital threats.
Our platform integrates ZTNA (Zero Trust Network Access), microsegmentation, endpoint protection, and identity-based segmentation, delivering a holistic approach to securing hybrid and multi-cloud environments.
Built on patented technology, TerraZone simplifies the implementation of Zero Trust principles by focusing on identity and device verification. This approach minimizes attack surfaces, prevents lateral movement, and ensures sensitive resources are only accessible to authorized users and devices.
Trusted by organizations in finance, telecom, healthcare, and government, TerraZone's platform provides advanced protection for critical infrastructures.
Our solutions are easy to deploy, highly scalable, and designed to support businesses as they innovate and grow securely.
With TerraZone, organizations gain a resilient cybersecurity framework powered by patented technology, ensuring data integrity, compliance, and a secure path to the future.

CATEGORIES:

- Application and Website Security
- Network Security
- Data Protection Encryption and Privacy
- End Point Security
- IoT
- Medical IoT

www.tonicsecurity.com

Enter the era of Contextualized Security.

Tonic is the Contextualized Security company. We provide a new way to accelerate triage, prioritization and remediation of vulnerabilities and threats. Our data fabric and advanced AI extracts meaningful and actionable context from unstructured company knowledge, super-charging vulnerability management and security operations.

CATEGORIES:

- GRC and Vulnerability Management
- Security Operations and Orchestration
- AI

Stop Fraud. Eliminate identity silos, security gaps and complexity

Transmit Security has reimagined fraud prevention and CIAM by replacing siloed solutions with a fusion of customer identity management, identity verification and fraud prevention. Mosaic by Transmit Security, the company's flagship platform, offers best-of-breed modular services to address fraud and identity use cases while minimizing complexity and costs. With AI-driven cybersecurity at its core, Mosaic is built for resilience and scale, earning the trust of 7 'top 10' US banks and Fortune 500s.

Solution: Mosaic by Transmit Security eliminates complexity, identity silos and security gaps as the only platform with a fusion of native fraud prevention, identity verification and customer identity management.

With a powerful fraud engine and layers of orchestrated services, this AI-driven platform automates context-aware decisioning that adapts journeys to mitigate risk or remove friction for trusted customers in real time.

Built for resiliency, scale and agility, Mosaic ensures business continuity and availability for millions of users while AI workflow automations optimize efficiencies for all internal stakeholders.

CATEGORIES:

- Anti-Fraud, Authentication and IAM
- CIAM (Customer Identity and Access Management)
- Fraud Prevention
- Identity Resiliency
- Fraud and Risk Management
- Identity Orchestration

AI Digital Employee for A-to-Z Identity and Access Management (IAM) tasks execution

Twine builds digital cybersecurity employees who execute tasks from A to Z to help cyber teams close the talent gap. The company's first digital employee, Alex, learns, understands and takes away the burden of identity management tasks - proactively completing the organization's cyber objectives. Twine was founded in 2024 by Benny Porat, Omri Green, Justin Woody and Nadav Erez, all former top managers at cyber unicorn Claroty, which was co-founded by Porat in 2015.

CATEGORIES:

- Anti fraud
- Uthentication and IAM
- AI
- Identity and Access Management

Waterfall Security Solution Enabling critical OT

Waterfall Security Solution 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.

CATEGORIES:

• OT & Industrial Control System

THE ISRAELI EVENT **AT RSA**

April 28, 2025 | SAN FRANCISCO
10 AM-5 PM

Production: IEICI Media and Communication Division | Design: Nurit shelach

www.export.gov.il