ISRAEL CYBER ALLIANCE

ISRAEL EXPORT INSTITUTE

Cyber Israel
Prime Minister Office
National Cyber Directorate

Ministry of Economy and Industry
Foreign Trade Administration

ISRAEL
Inspired by *innovation*

Israeli Cyber Security Solutions for Business Continuity

The Israel Cyber Alliance

The Israel Cyber Alliance (ILCA), a joint venture between the Israel Export Institute, the Ministry of Economy and Industry, and the Israel National Cyber Directorate, represents more than 350 Israeli companies in the cyber security field, and works to maximize the markets. ILCA exposes Israeli capabilities and innovative cyber security solutions to potential foreign clients and partners, either as stand-alone solutions or as an overarching tailor-made suite of solutions, accommodating their specific short- and long-term needs. To that end, ILCA, which plays a key role in the Israeli ecosystem and is well acquainted with the needs of the local cyber industry, holds the most comprehensive and up-to-date database of Israeli-based cyber security companies.

ILCA's wide and global network of partnerships with foreign counterparts, from the public and private sectors alike, is constantly exploring new avenues of cooperation with its existing partners. Additionally, ILCA is looking to expand its network and forge new productive partnerships with foreign governments and organizations, in order to generate substantial business value both for its Israeli members and for its foreign counterparts and partners.

For more information, please contact:

Ms. Yaara Sabzerou - Manager, Cyber Security | Israel Export Institute | yaaras@export.gov.il

Mr. Gal Givon- Marketing Coordinator, Cyber Security | Israel Export Institute | Galg@export.gov.il

Ms. May Bar Marketing Coordinator, Cyber Security | Israel Export Institute | Mayb@export.gov.il

https://israelcyberalliance.com/

Content

Automated Pen-Test

Automotive Security

Behavioral Analytics & Threat Detection

Cloud Security

Consulting &Training

Data Protection, Security & Encryption

Endpoint Protection and EDR

GRC, Risk and Posture

Content

Identity Management & Fraud Detection

Incident Management & Response + Orchestration

IoT Security + IIOT

Network Security

OT Security & SCADA

Threat Intelligence

Web Application & Security

CYE

CYE provides cyber security assessment and maturity improvement program by combining Human and Machine intelligence

www.cyesec.com

Categories

- Security Assessments
- Red Team
- Breach and attack simulations
- Penetration testing
- Incident response

Profile

Founded in 2012 with offices in the US and Europe, CYE offers cyber security assessments and unique cyber maturity improvement program using combination of human experts and artificial intelligence technology.

Together with CYE's dynamic mitigation plan program, organizations can remain focus solving the prioritized cyber risks. Continuous assessments coupled with regular mitigation plans, help increase security yet decrease the use of scarce resources.

Solution at a Glance

CYE goal is to support organizations become more cyber security mature in a continuous process which includes using the company resources in the most cost effect way.

The security posture assessment is done by combination of nation level expert and "Hyver" – a virtual hacker technology coupled with managed international community of white hat experts.

Use Case

The outcome of the continuous assessment allows to view, using graph analytics, the critical attack routes from the initial attack positions (internal, external, etc.) and the business-critical assets CYE was able to get access to.

Using predictive analytics CYE is able to create mathematical proven mitigation plan which provide the most cost-effective way of using the organization resources to improve the posture.

Return to Content
Slide 3

Cymulate

Breach and Attack Simulation

www.cymulate.com

Categories

- Breach and Attack Simulation
- Automated Penetration Testing

Profile

Cymulate is a SaaS-based breach and attack simulation platform that makes it simple to test, measure and optimize the effectiveness of your security controls from anywhere, any time, all the time. With just a few clicks, Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you're exposed and provide remediation guidance—making security continuous, fast and part of every-day activities. With Cymulate you can perform comprehensive security assessments, on your production network without risk of disruption

Solution at a Glance

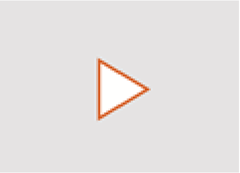
Easy to deploy, simple to use and automated Cymulate requires either one or no agent for testing. Integration with leading SIEM, EDR and vulnerability scanner systems enhance the value of your existing security programs. Updated daily be Cymulate security researchers, blue teams can continuously check their defenses against the latest attacks, while customization enables red teams to automate and repeat their attack scenarios.

Use Case

Our customers use our platform to:

- Measure and track their cyber posture
- Validate and improve security control effectiveness
- Test against the latest threats, updated daily.
- Discover and fix infrastructure misconfigurations that enable a hacker to move laterally within their network
- Uncover 3rd party supply chain security weaknesses
- Test SOC and SIEM's ability to detect an attack

video



Return to Content Slide 3

Pcysys

Automated Penetration Testing with a Click of a Button

www.pcysys.com

Categories

Automated Penetration Testing

Risk Management

Profile

Pcysys delivers PenTera, the automated network penetration testing platform that assesses and helps reduce corporate cybersecurity risks. Hundreds of security professionals and service providers around the world use PenTera to perform continuous, machine-based penetration tests that improve their immunity against cyber-attacks across their organizational networks. With leading investors, AWZ Ventures and the Blackstone Group, and over 100 enterprise global customers across all industries, Pcysys is the fastest-growing cybersecurity startup in Israel.

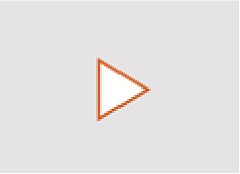
Solution at a Glance

Requiring no agents or pre-installations, the PenTera™ platform scans and ethically penetrates the network with the latest hacking techniques, prioritizing remediation efforts with a threat-facing perspective. With PenTera™, a company can maintain the highest resilience posture by performing penetration tests as frequently as needed. The PenTera platform covers the scope of what is nowadays managed by several separate tools, including vulnerability assessment, security control validation, credential strength validation, network equipment testing, and privileged access audits.

Use Case

Whether installed on-site or on the Cloud, PenTera is run remotely allowing organizations to continuously test and validate their security controls from the attacker's perspective, on-demand. The platform weighs each weakness as part of the complete attack vector to better prioritize remediation efforts, instantly providing a complete pentesting report. This enables security executives to constantly align with the changing business needs and the evolving attack surface. Pentesting is turning into a remote daily activity. For more information click here.

video



Return to Content Slide 3

XM Cyber

Defense by Offense

www.xmcyber.com

Categories

Breach and Attack Simulation

Automated Pen Testing

Cloud Security Posture Management

Cyber Attack Modeling

Profile

XM Cyber was founded by security executives from the elite Israeli intelligence sector. XM Cyber’s core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security. XM Cyber gives you the ability to see your network the way the hacker sees it. It helps you to find all existing hidden vectors of attack, including those that typically go under the radar of most protective measures. And once an attack path is identified, XM Cyber delivers a focused and prioritized remediation report so you can fix those weaknesses before the hacker strikes.

Solution at a Glance

XM Cyber is the only available Breach and Attack Simulation software solution that safely simulates an advanced persistent threat (APT) against your organization’s critical assets. Our patented approach helps you reduce your risk by exposing gaps resulting from unpatched systems, misconfigurations, software flaws and human error.

Use Case

Automated Red Team. Enable any team with the ability to see how an attacker would traverse to a crown jewel regardless of red team expertise. Simply pick an asset and the attacks are calculated automatically.

Continuous Validation. Networks are dynamic and so should be the testing. XM Cyber enables continuous validation of risk to your assets as your network evolves.

Return to Content
Slide 3

Cylus

Cybersecurity on Track

www.cylus.com

Categories

Railway Cybersecurity
Transportation Cybersecurity

Profile

Cylus, the global leader in rail cybersecurity, helps mainline and urban railway companies avoid safety incidents and service disruptions caused by cyber-attacks. Led by veterans from the Israel Defense Forces' Elite Technological Unit together with top executives from the railway industry, Cylus combines deep expertise in cybersecurity and rail.

Solution at a Glance

Cylus created CylusOne™ – the first-to-market cybersecurity solution that meets the unique needs of rail, mainline and urban. Cylus' software-based solution provides unprecedented visibility into the signaling and control networks – wayside and onboard – instantly detecting malicious activities. Alerts are supplemented with actionable insights, facilitating an effective response

Use Case

Cylus monitors a variety of railway-specific networks and is the only company to offer a comprehensive solution for rail systems such as signaling, onboard and train communications. An example can be the monitoring of a complete ERTMS network, including the field elements, the ETCS communications and the GSM-R.

Return to Content
Slide 3

Upstream Security

Making smart mobility safe and secure. For everyone.

www.upstream.auto

Categories

Smart Mobility

Profile

Upstream Security is the first cloud-based cybersecurity solution purpose-built for protecting connected vehicles and smart mobility services from cyber-threats and misuse. Upstream's C4 platform leverages existing automotive data feeds to detect threats in real-time and delivers cybersecurity insights supported by AutoThreat Intelligence, the first automotive cybersecurity threat feed in the industry.

Solution at a Glance

Upstream improves the safety and security of connected vehicles and services built around them by monitoring business critical events and identifying cyber threats in real-time via a centralized cloud-based analysis of multiple automotive data feeds, including telematics and mobile applications. The solution is 100% agent-less and does not require any hardware or software inside the vehicles. Upstream's solution is already used by millions of vehicles worldwide, providing an effective and innovative method in detecting threat anomalies and mission critical events using a combination of machine learning, cybersecurity engines, and service policy enforcement.

Use Case

- Machine learning based profiling and anomaly detection
- Protects against known and unknown cyber threats
- Provides SOC teams and analysts with visibility and insights
- Automated and custom service policies
- Triage and root-cause analysis

video

Return to Content Slide 3

Hunters

Autonomous Threat Hunting

https://hunters.ai/

Categories

Extended Threat Detection and Response - ‘XDR’

Threat Hunting

SOC Automation

Profile

Hunters launched its innovative autonomous threat hunting solution in May 2019, to enable organizations hunt threats at scale, and stop attacks at their root. Combining unique attack intelligence and AI, ‘Hunters.AI’ scales top-tier threat hunting techniques and detects cyber attacks that bypass existing security solutions.

Solution at a Glance

By seamlessly connecting to raw organizational data and extracting TTP-based threat signals, Hunters.AI performs autonomous investigation and intelligently correlates signals across all IT environments. Hunters.AI equips security operation teams with bottom-line attack stories, enabling rapid identification, comprehension, and response to newly exposed cyber threats.

Use Case

Extend detection through automation. Use Hunters.AI to face against attack efficacy and the scarcity in cyber-adversary expertise. While SOC processes remain analyst-centric, attack detection cannot and should not afford the wait.

Empower your SOC. Use Hunters.AI’ interconnected threat analysis to rise above threat telemetry noise and manual processes.

Embrace your data. Cyber attackers blend in the noise. Utilize AI to embrace every bit of data and find their traces. Now is the time to do it at scale.

video

Return to Content
Slide 3

Guardicore

Say Goodbye to Legacy Firewall Complexity

https://www.guardicore.com/

Categories

- Reduce Complexity with an infrastructure-agnostic approach
- Reduce Risk with granular segmentation policies that prevent lateral movement within your data center and cloud environments.
- Innovate Faster by integrating security into DevOps and IT automation workflows

Profile

Guardicore is an innovator in data center and cloud security that protects your organization's critical assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security — for any application, in any IT environment. Guardicore was founded in 2013 with the goal of reinventing security to place greater emphasis on security beyond the traditional network perimeter.

Solution at a Glance

The Guardicore Centra Security Platform makes visualizing and securing on-premises and cloud workloads fast and simple. It creates human-readable views of your complete infrastructure – from the data center to the cloud – with fast and intuitive workflows for segmentation policy creation.

Use Case

How do you build a good segmentation policy? Instead of using multiple policy management tools such as Firewalls, VLANs, ACLs, or cloud security groups, Guardicore offers a single segmentation policy for the whole environment from a single console.

https://www.guardicore.com/covid-19/

video

Return to Content
Slide 3

Cybint

A Cyber Education Company

www.cybintsolutions.com

Categories

Cyber Education; Cybersecurity Simulation; Workforce Development

Profile

Cybint is an international cybersecurity education company that focus on the human factor at all levels of expertise. Cybint solves two of the biggest cybersecurity challenges – The workforce shortage and skills gap, by partnering with education institutions to launch cyber training centers and boot-camps worldwide; and by providing cyber training and simulation platforms for corporations and government agencies to protect against emerging cyber threats.

Solution at a Glance

Cybint’s Bootcamp is designed to train learners without prior experience in cybersecurity to entry level security positions. They will learn latest content through Cybint’s platform that will allow them to self-pace their learning.

They will have the in-person support of a local trainer which will be trained by Cybint, to help them with specific challenges and a cohort of classmates will make the learning process more engaging.

Use Case

Cybint’s internationally successful Cyber Bootcamp program prepares learners for success in the job market by equipping them with practical industry expertise and soft skills, according to the leading skills framework for cybersecurity workforce development.

Return to Content Slide 3

BitDam

Stop unknown threats at first sight

www.bitdam.com

Categories

Data Protection, Security & Encryption

Profile

BitDam is a pioneer in cyber defense, securing enterprise email, cloud drives and other collaboration tools from ransomware, malware and phishing. Recognized by Frost & Sullivan for its technology leadership, BitDam's award-winning ATP solution is utilized by hundreds of thousands of end-users and deployed by leading organizations in Europe and the US, with a proven record of detecting threats that other security solutions fail to uncover.

Solution at a Glance

BitDam ATP protects email (Office 365, G-Suite, MS Exchange), cloud drives (OneDrive, G-Drive, Dropbox, Box) and enterprise messaging (Teams, Slack). Unlike the alternatives that give a "grace period" to unknown cyberthreats, BitDam's attack-agnostic cloud-based solution stops malicious files and URLs at first encounter with unprecedented detection rates, empowering organizations to collaborate safely.

Use Case

BitDam realizes the importance of keeping all enterprise communication channels protected from unwanted threats in these vulnerable times, with many of us reliant on working remotely, working with Microsoft Teams, OneDrive and so on.
To support organizations in these challenging times, we offer BitDam ATP for Microsoft Teams for free for a period of 3 months and provide a free 1-month trial for BitDam ATP for OneDrive.

video

Return to Content
Slide 3

ITsMine Beyond DLP™

Protect data within company boundaries and beyond

www.ITsMine.io

Categories

Beyond DLP
DLP
Data Loss Prevention
Deception
Ransomware protection
End Point protection
Data breach detection
Data protection
GDPR / CCPA / HIPAA

Profile

ITsMine’s Beyond DLP™ - Data Loss Prevention solution enables organizations to proactively protect against internal and external threats, automatically. The product alerts and gives critical forensic information even after data exfiltration beyond companies boundaries. ITsMine is easy to implement, meets regulatory requirements, is transparent to employees and IT teams and requires no permanent endpoint agents

Solution at a Glance

The solution solves the DLP challenge utilizing artificial intelligence, behavior analysis, and deception techniques. ITsMine secures and protects all stages of digital data (at rest, in motion and in use), without requiring policies or permanent endpoint agents, thus having no effect on employee productivity. Additionally, ITsMine has negligible false positives.

Use Case

External attacker: When an external attacker on managed or unmanaged device harm or steal data. Beyond DLP automatically blocks and isolates the compromised endpoint, and provides important forensic information even after data exfiltration. Internal Employee: Intentional or unintentional misuse, exposure to or the harming of company data by an employee. ITsMine empowers employees to handle critical data with the proper care. By detecting abnormal behavior and calculating risk levels, the solution can automatically educate, block activity, or send unparalleled information obtained on the employee’s suspicious activity to your security department.

video

Return to Content Slide 3

Safe-T Data

Allow Everything. Trust Nothing.

www.safe-t.com

Categories

- Zero Trust
- Software Defined Perimeter
- Zero trust network access (ZTNA)

Profile

Safe-T Data is a provider of access solutions which mitigate attacks on enterprises' business-critical services and sensitive data, while ensuring uninterrupted business continuity. Safe-T's cloud and on-premises solutions ensure that an organization's access use cases, whether into the organization or from the organization out to the internet, are secured according to the "validate first, access later" philosophy of zero trust. This means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network or in the cloud. Safe-T's wide range of access solutions reduce organizations' attack surface and improve their ability to defend against modern cyberthreats.

Solution at a Glance

Safe-T's Zero Trust Network Access (ZTNA) solution, Secure Application Access, is changing the way organizations grant secure external access to their services. It offers secure and transparent access for all types of entities to any internal application, service and data. The solution implements Safe-T's patented reverse-acces technology which eliminates the need to open incoming ports in the organization's firewall. Safe-T Secure Application Access forces users to authenticate into resources first and then they are granted access by the solution.

Use Case

- Connect remote employees to the network
- Connect third party vendors to specific applications

video

Return to Content
Slide 3

Sasa Software

Medical Imaging Security in the COVID-19 reality

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

Categories

Secure telehealth

DICOM Security

Advanced Threat (APT) Prevention

OT/ICS Security

Profile

Sasa Software is a leading provider of Content Disarm and Reconstruction (CDR) solutions. GateScanner® CDR is a proven, award winning technology, protecting healthcare organizations, financial/insurance institutions, governmental agencies, and public utilities. Primary use cases are: Medical Imaging (DICOM), Portable (USB) media security, email, document uploads, browser downloads, network separation, and security for other content delivery routes.

Solution at a Glance

GateScanner CDR prevents advanced and undetectable file-based attacks including zero-days, exploits and ransomware using best of breed detection technologies, and proprietary file disarm to transform every incoming email and file into a neutralized (harmless) copy, while maintaining full file fidelity, visibility and usability.

Use Case

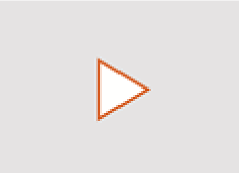
Enable secure telehealth for medical imaging:

In the COVID-19 reality patients are restricted from entering medical facilities but still need to deliver imaging test results. GateScanner DICOM Protector enables remote uploads of imaging results while ensuring files delivered are threat-free.

Read about DICOM vulnerabilities here

And about GateScanner DICOM protector here

video



Return to Content
Slide 3

Comsec Global

COMSEC

www.comsecglobal.com

Categories

Cybersecurity Consulting Services

Profile

Tap into over 32 years of cybersecurity consultancy experience with a proven track record of success. With millions of data points being compromised every day, your organization must stay continuously resilient to cyber threats. Comsec Global's advisors deliver innovative services to secure your information and operational assets, ensuring long term business results.

Join the 1,000+ leading companies in over 40 countries and across 5 continents that trust Comsec Global.

Solution at a Glance

Trusted by Fortune 500 companies and startups in a diverse range of verticals: Government, Finance, Insurance, Healthcare, Telecommunication, Ecommerce, Gaming, Industrial, Logistics, Public transportation. Secure your information and operational assets with the broadest portfolio of cybersecurity services. All our consultants are certified in specific niche markets. All have spent years building expertise and are fully immersed in their niches.

Use Case

The attack surface is expanding and the climate for cyber-attacks is rapidly evolving as organizations scramble to move their activities online to protect their employees and maintain business continuity in the face of COVID-19.

With hackers looking to capitalize on opportunities in this new reality, organizations are exposed to a broader range of potential threats than ever before.

Return to Content
Slide 3

ContextSpace Solutions Ltd

Revolutionizing Privacy

www.contextspace.com

Categories

Privacy Compliance Enforcement

Data Protection by Design and by Default

Profile

Intrinsic Privacy Technology® from ContextSpace enables organisations to enforce data protection compliance across all digitally-enabled applications, processes and products.
Our innovative approach to compliance enforcement cuts through organizational and technical obstacles to produce sustainable privacy compliance at lower effort, skills and cost.

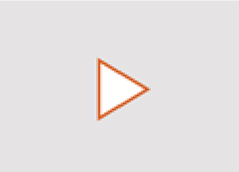
Solution at a Glance

- **Privacy Designer** enables step-by-step collaboration when assessing purpose, scope and risk for digital apps and IoT.
- **Privacy Center / DSAR** automates self-service fulfillment for data subject rights and Subject Access Requests.
- **Data Protection By Design / DPbD** provides privacy-enabled APIs, big-data encryption and other data protection services.

Use Case

- A bank must to comply with GDPR and uses **Privacy Designer** to model lawful processing, data scope and risks.
- The bank deploys **Privacy Center** portal and self-service processes for subject data rights and data access requests.
- Since GDPR requires ”data protection by design”, the bank employs **DPbD** technology for developing new applications and transforming its legacy systems for compliance.

video



Return to Content Slide 3

Maya Security

Business, Secure

https://www.maya-security.com/

Categories

Cybersecurity

Board Advisory

Strategic Cybersecurity

Cyber Resilience

Profile

Maya was founded in late 2012 with one main goal – bridging the inherent gap between senior management, the IT department and Information Security to promote successful business processes through better Cybersecurity.

Maya works with decision makers to manage cyber-risk, in an informed manner and in collaboration with the company CISO and CIO.

Solution at a Glance

With business slowing down and uncertainty growing, this is the time to be proactive in enhancing cybersecurity across the company, protecting it from existing and new risk.

As cybercriminals are exploiting the coronavirus crisis t o cash in on uncertainty and the global shift to teleworking

Maya Security is working to protect companies right now and prepare them for the days after the crisis is over.

Use Case

Maya works with management and the board of directors to align the company's cybersecurity strategy to the business strategy. Finding creative solutions to meet to company's budget, corporate culture, existing technical skillset and management preferences.

Maya discovers the company's threat landscape, possible gaps in risk mitigation and works with the company to mitigate the cyber-risk it faces.

Return to Content
Slide 3

Panorays

Automated third-party security

https://www.panorays.com/

Categories

Third-party security risk management

Cybersecurity ratings

Profile

Panorays automates third-party security lifecycle management.

With the Panorays platform, companies dramatically speed up their third-party security evaluation process and gain continuous visibility while ensuring compliance to regulations such as GDPR, CCPA and NYDFS. It is the only platform that enables companies to easily view, manage and engage on the security posture of their third parties, vendors, suppliers and business partners. Panorays is 100% SaaS, no installation needed.

Solution at a Glance

Panorays provides a 360-degree rating that combines an overview of your vendor’s attack surface with the automation of a smart, customized security questionnaire. Using Panorays, organizations receive these benefits:

Rapid supplier evaluation. Customers typically receive responses from vendors within eight days.

Clear remediation plans. Find out what your suppliers’ cyber gaps are and how they can close them.

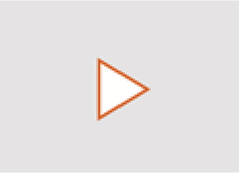
Continuous monitoring with live updates about any changes to cyber posture.

Use Case

Because of coronavirus, suppliers are shifting to a mass remote workforce. This sudden transition is creating significant cybersecurity challenges, including an increase in supply chain attacks**.**

Panorays helps ensure that your suppliers’ cybersecurity is ready for these challenges through its **COVID-19 security questionnaire.** The automation of the questionnaire enables you to scale your process, so you can quickly find out if your suppliers have the necessary policies in place to support a remote workforce.

video



Return to Content
Slide 3

PRIMESEC

Connecting between technology and law

https://www.primesec.co.il/t-en-us

Categories

Information security consulting, privacy and cyber protection

Profile

Primesec is a private owned consulting company to organizations regarding IT legislation and regulations, information security, GDPR, Cloud security BCP DRP and IT management. Since its establishment, the company provides solutions in these spheres, while taking into consideration the needs of the organization and its business while interacting with its business and organizational processes.

Solution at a Glance

Primesec approach is of an educated combination of the regulatory demands for the organization and its characterization, while combining between the different regulations in order to produce an effective compliance process.

Use Case

Our main value is a fast, professional and adequate response to the information security, regulatory and technology needs of our customers. We believe that staying on schedule and providing our customers with personal and continuous attention will allow us to provide and respond a fast, efficient and qualitative solutions for their immediate events and needs.

Return to Content
Slide 3

Vicarius

Patch-less Vulnerability Management

www.vicarius.io

Categories

Vulnerability Management

Patch Management

Risk-Based Vulnerability Management

Virtual Patching

Profile

Vicarius helps SMEs protect critical apps and assets against software exploitation with the world's first all-in-one vulnerability management platform designed for CISOs, MSSPs and IT Admins. Backed by JVP and E.ON, Vicarius's mission is to provide today's organizations with powerful solutions that ensure regulatory compliance and top-tier, military-grade cyber protection.

Solution at a Glance

TOPIA analyzes, prioritizes and protects third-party apps against threats and attacks.

Manage your organization's security cycle from start to finish and protect more, faster by focusing on the threats that matter most.

Use Case

TOPIA’s Patchless Protection - Thanks to TOPIA, Mandel Foundation now completes the patching process within 12 hours when it used to take us much longer.

xTags - TOPIA’s risk-analysis engine helped JCE identify up to 32 high-risk applications that were vulnerable to exploitation.

video

Return to Content
Slide 3

nsKnox

Corporate Payment Security

https://nsknox.net/

Categories

Corporate Payment Security

B2B Payment Protection

Anti-Fraud

Profile

nsKnox is a cyber-fintech company focused on Corporate Payment Security, founded and led by Alon Cohen, Founder & former CEO of CyberArk (NASDAQ: CYBR).

Backed by Microsoft Ventures, Viola Ventures and IDB Bank, nsKnox is based in New York, London and Tel Aviv.

Solution at a Glance

nsKnox solutions protect corporations and banks against cyber-fraud carried out by insiders or outsiders, preventing significant financial losses and reputational damage.

Leveraging its groundbreaking Cooperative Cyber Security™ (CCS) technology to combine the cyber strength of multiple organizations, nsKnox's solutions detect and prevent finance & ops infrastructure attacks, social engineering, business email compromise (BEC) and other Advanced Persistent Fraud attacks.

Use Case

A multi-billion-dollar, global media giant with hundreds of locations worldwide conducts business with thousands of suppliers and executes payment transactions from multiple and distributed finance centers.
PaymentKnox has enabled the media giant to increase the accuracy and efficiency of its bank account validation processes, secure its payments and prevent internal fraud, IT-level malware attacks on corporate payment systems, and social engineering attacks

video

Return to Content
Slide 3

Secret Double Octopus

Liberating Businesses From the Pains of Passwords

https://doubleoctopus.com/

Categories

Authentication

Profile

Secret Double Octopus delights end users and security teams alike by replacing passwords across the enterprise with the simplicity and security of strong passwordless authentication.

Our unique, innovative approach provides users with a simple “touch and go” experience and a consistent way to access applications while providing stronger protection against cyber-attacks, ensuring users and IT teams never have to remember or use another password.

Solution at a Glance

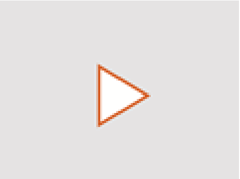
Our solution enables organizations to benefit from high assurance passwordless access to domain accounts, cloud and SaaS applications, networks and most legacy applications.

For password-based systems such as AD, our innovative solution swaps user managed passwords with machine-generated keys, and protects them with a more secure multi-factor authentication process.

Use Case

Especially for remote workers, organizations gain the benefits of centrally-controlled high assurance identities across domain accounts, VPN, cloud applications and virtually all legacy applications. To connect to the enterprise VPN, users simply tap the Octopus Authenticator on their mobile device and identify biometrically. The Octopus Authenticator implements provably unbreakable cryptography that is highly resistant to common attacks such MitM and cracking, while ensuring protection against phishing and user manipulation.

video



Return to Content
Slide 3

Silverfort

Enabling Secure Authentication and Access Without Agents or Proxies!

www.Silvefort.com

Categories

Multi-Factor Authentication and Access Policies

Secure Privileged Access and Use of Service Accounts

Holistic Zero Trust Policy Enforcement

Profile

Silverfort delivers secure authentication and Zero Trust policies across corporate networks and cloud environments, and within these environments, without deploying any software agents or inline proxies. Using patent-pending technology, Silverfort enables risk-based multi-factor authentication for all sensitive users, devices and resources, including systems that could not be protected until today, such as homegrown applications, IT infrastructure, file systems, machine-to-machine access and more.

Solution at a Glance

Silverfort introduces a revolutionary new approach that enables enforcement of secure authentication and access policies in a holistic and non-intrusive way. By seamlessly applying a layer of protection on top of existing authentication protocols, Silverfort eliminates the need to deploy agents or proxies, or to change existing servers and applications. This enables organizations to protect any sensitive asset without having to modify it, and to extend protection to interfaces that are not covered by any other MFA solution.

Use Case

- Secure remote access anywhere!
- Agentless Multi-Factor Authentication for sensitive systems that couldn’t be protected until today
- Holistic enforcement of Zero Trust policies, not just at the perimeter but within the network segments themselves
- Secure privileged access and service accounts
- Enabling secure migration of homegrown and legacy apps to the cloud
- Enforcing adaptive risk-based authentication policies

video

Return to Content Slide 3

Transmit Security

Simplify, accelerate, and reduce the cost of identity projects

https://www.transmitsecurity.com/

Categories

- Identity and Access Management
- Fraud and Risk Reduction

Profile

Transmit is the leader in Identity Orchestration. Our technology enables large enterprises to standardize and simplify their identity infrastructure to accelerate and reduce the cost of new account opening, authentication, authorization, compliance and fraud prevention related initiatives. Transmit Security's founders created Trusteer (now IBM Security) and Imperva (IMPV on NYSE). Transmit Security funded in 2014, and based in Boston and research and development in Tel-Aviv.

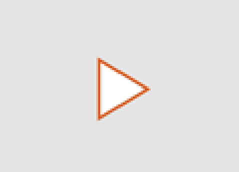
Solution at a Glance

Transmit Security is a cross-channel orchestration platform provider that abstracts identity, authentication, authorization, and user-risk decisioning. An extensible plug-and-play platform consolidates existing solutions to simplify, reduce cost, and speed deployment of identity-related programs. Continuous scoring combines risk data with user, device and system profiling for real-time decisioning at every step, across every system.

Use Case

Transmit covers many customer and workforce identity, authentication and trust management use cases. For organizations with large customer base operations, Transmit offers solutions for new account opening, account authentication, transaction signing, biometric authentication, behavioral threat detection and many more. Enterprise workforce solutions include passwordless account login, multi-factor authentication, access management, soft-tokens, single-sign on, and directory services.

video



Return to Content
Slide 3

Cynamics

Unlimited Visibility & Unprecedented Scalability for Smart Networks

www.cynamics.ai

Categories

Network Performance Monitoring and Diagnostics

Network Security

Profile

Cynamics, a network monitoring and cybersecurity solution that’s giving Local Governments, Municipalities, and Critical Infrastructure providers an unlimited visibility into their networks, to optimize network performance and predict cyber-attacks including ransomware. The solution uses patented Artificial Intelligence (AI) and Machine Learning to accurately predict attacks and infer complete network visibility at scale. That’s a big deal because current monitoring tools leave dangerous blind spots in areas where there’s no network coverage, allowing threats to infiltrate. But what makes the solution unique is the fact that it provides this total, holistic view at a fraction of the cost of current solutions on the market.

Solution at a Glance

Cynamics SaaS based solution collects small network traffic’ samples, specifically, packet header details, such as IP addresses, port numbers, protocol, length, geo location, etc.
Cynamics algorithms infer the complete network performance and automatically digest the traffic behavior at every timestamp, comparing to its historical values and trends and looking for suspicious patterns. When attack or anomaly is detected, Cynamics’ provides strong analysis capabilities in order to further investigate the threat severity and risk.

Use Case

Fayette County has added Cynamics as a new layer of network visibility and protection to the growing threat of potential cyberattacks. The solution’ onboarding took less than a hour and right after the implementation the Customer could see for the first time the complete interconnected network of the entire county. Since Cynamics technology relies on standard sampling protocols which are built into the existing network devices: Switches, Routers, Firewalls, etc. Cynamics is non intrusive and risk free. In particular, no appliances or agents installation is needed.

Return to Content
Slide 3

Intezer

We identify the origins of code

https://intezer.com/

Categories

Cloud Workload Protection

Malware Analysis

video

Return to Content Slide 3

Profile

Intezer introduces a Genetic Malware Analysis technology, revolutionizing cyber threat detection and response. By revealing the origins of software code, Intezer equips enterprises with an advanced way to detect modern cyber threats, while providing deep context on how to effectively respond to incidents. Intezer offers solutions for incident response automation, cloud workload protection, threat intelligence, and more.

Solution at a Glance

Intezer Protect: Protect your cloud workloads in runtime against unauthorized and malicious code Gain visibility and control over every fragment of code running on your cloud infrastructure

Intezer Analyze: Automate your Security Operations and Incident Response with Genetic Malware Analysis. Quickly analyze files and devices to immediately understand the What, Who, & How of a potential cyber incident, by identifying even the smallest pieces of code reuse

Use Case

Regardless of the chosen attack vector or surface, a cyber attack is almost always the result of some piece of code running in memory. That’s why we believe the key to mitigating cyber attacks must be to identify the core of all attacks: malicious code. Deeply analyzing the actual binary code, whether on disk or in-memory, allows us to help you detect modern and sophisticated threats, while providing deep context on how to properly respond to incidents.

ZecOps

Automated Digital Forensics

www.zecops.com

Categories

Security Automation

Endpoint, Server, and Mobile Security

Forensics Automation

Profile

ZecOps delivers a realistic take on cyber security with an agentless Digital Forensics and Incident Response (DFIR) platform. ZecOps enables automated discovery, analysis, and disinfection of persistent attacks that go unnoticed by existing security controls by finding and leveraging attackers' mistakes. The platform is suitable for endpoints, servers, mobile devices, and other embedded devices. ZecOps founders and core team are renowned entrepreneurs and cyber security veterans. The company is headquartered in San Francisco and has offices in Tel Aviv, Buenos Aires, Singapore and London.

Solution at a Glance

Zecops platform detects attackers' mistakes in order to:

- Provide organizations with an immediate view on which assets are compromised
- Automatically produce threat intelligence from existing attacks

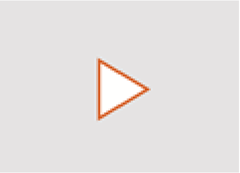
The platform provides:

- Continuous digital forensics
- Automated compromise and risk assessment
- Investigation time reduction from months to minutes

Use Case

- Detect past and ongoing cyber espionage campaigns on organizations' devices
- Identify compromised assets
- Increase systems' operational availability on servers and endpoints
- Pre & Post travel inspections for executives, VIPs and employees with sensitive data

video



Return to Content Slide 3

Cynerio

Medical-First IoT Cybersecurity
Agentless. AI Powered. Actionable.
www.cynerio.com

Categories

Healthcare IoT cybersecurity

Cyber Risk Management

Profile

Cynerio is the world's premier medical-first IoT cybersecurity solution. We view cybersecurity as a standard part of patient care and provide healthcare delivery organizations with the insight and tools they need to secure clinical ecosystems and achieve long-term, scalable threat remediation without disrupting operations or the delivery of care.

Solution at a Glance

Cynerio's medical-first platform integrates seamlessly with healthcare network infrastructures, facilitates the alignment of biomed and IT security goals, and translates IT risk into business risk. Our intuitive UI includes interactive visualizations of network topography, vendor communications, device visibility, profiles, and vulnerabilities. Cynerio aligns hospitals' risk mitigation plans with business goals by providing robust segmentation policies that enable long-term and scalable threat remediation programs. View Solution Brochure

Use Case

Challenge: Reduce attack surfaces and cyber risk for hospitals using medical devices running unsupported OS without disrupting workflow or medical care.

Solution: Prioritize device risk according to clinical impact and hospital workflows so IT security teams can build and enforce policy that leverages existing security tools and network infrastructure.

Result: Effective microsegmentation policy that limits device connections and provides tools to respond to suspicious cyber events. View Use Case

video

Return to Content
Slide 3

Essence SigmaDots

Delivering the foundation for true IoT security and visibility

www.sigmadots.com

Categories

- Data Protection, Security & Encryption
- IoT & IIoT Security
- Network-Security

Profile

Essence SigmaDots, part of the Essence Group, a leading developer of connected devices and IoT platforms, with more than 45 million devices deployed worldwide, brings the power of embedded, distributed, and multilayered cybersecurity to the IoT ecosystem. Combining the creativity and agility of a startup with the experience of a market leader, our unique platform authenticates critical commands, safeguarding privacy, securing device communication, and ensuring cyber and operation visibility for IoT.

Solution at a Glance

Essence SigmaDots' holistic IoT cybersecurity solution, uses a fully-embedded, distributed, and multilayered approach with low-friction integration. Our patent pending solution: on-the-edge dynamic firewall and antivirus, distributed broker networking protocol and end-to-end encryption as a service, together with cloud-agnostic/on-premises cyber and operational visibility, protect IoT endpoints and networks, and reduces the risk of advanced IoT based attacks on backend services.

Use Case

The Essence SigmaDots' solution is easily deployed including after-market support, ensuring business continuity and resilience for both IoT manufacturers and service providers. Designed and built by experts in tailoring solutions for IoT environments, the SigmaDots platform protects against a wide array of cyber-threats, reducing the risk of production downtime, service disruption, regulatory fines, and damage to reputation.

video

Return to Content Slide 3

FirstPoint Mobile Guard

Secure cellular communications for any device

www.firstpoint-mg.com

Categories

Mobile security

IoT security

Profile

FirstPoint's cybersecurity system detects, alerts and protects against built-in vulnerabilities in 2G-5G mobile networks, including fake cell towers, system loopholes, malicious & binary SMS, malware, backdoors and more.

Solution at a Glance

Our cellular network-based approach is managed by the organization with per device profiling. Transparent to the user/device and agentless, thus increasing user adoption.

Use Case

Protecting against communication interception, DoS, account hijacking, data leakage, location tracking, for mobiles, critical infrastructure, connected cars, payment terminals, smart cities and more.

video

Return to Content
Slide 3

SecuriThings

Managing IoT Operations at Scale

www.securitings.com

Categories

Risk detection
Endpoint protection capabilities

Predictive maintenance
Real-time health monitoring

Automated operations
Mitigation & maintenance

Profile

SecuriThings is a leading IoT technology provider, helping organizations maximize their security and operational efficiency when managing IoT at scale. The company's solution, Horizon, has been deployed in major airports, universities, cities, and large enterprises, and is already monitoring millions of devices globally. SecuriThings has established partnerships with world-leading global system integrators, device management systems and edge device vendors.

Solution at a Glance

SecuriThings Horizon is the first IoTOps solution to provide risk detection, predictive maintenance and automated operations, in one unified view.
The software-only solution is seamlessly and remotely deploying endpoint protection and health monitoring capabilities to each supported IoT device.
Using Horizon, organizations can now automate their cyber security and maintenance policies.

Use Case

Deploying Horizon, physical security teams in airports, universities or corporate campuses benefit from edge visibility and control over thousands of video surveillance and access control devices.
They can detect and mitigate cyber-threats, and drive predictive maintenance on new and existing devices, in an automated manner.

video

Return to Content
Slide 3

Terafence ltd.

Impenetrable Shield For IoT Devices

www.terafence.com

Categories

IoT security

Profile

Terafence is a startup company established in late 2015, and behind it are content professionals in the fields of communications, satellite, engineering, programming, and medicine.

Terafence has unique products that rely on innovative capability and absolute control (and smart) of data flow direction, safely and completely isolated without the possibility of hacking and/or interrupting the data flow.

Solution at a Glance

Terafence's hardware-based technology, “smart-wire”, offers a solution that maintains data flow of IoT devices, while physically isolating them from all types of cyber threats. The technology acts as a physical barrier that segments and isolates IP-enabled devices, while maintaining data flow direction and control intact. Terafence's hardware based FPGA solution, does not have an IP address, OS, operating system, or CPU to negotiate passage through. Terafence “smart-wire” is completely transparent to the network.

Use Case

- Israeli Defense Force projects
- Water utilities
- US – HLS/Security as a service provider (IP cams)
- Italian OEM (Smart machines/Industry4)
- Indian government (IP cams)
- CRIWare Japan partner

video

Return to Content
Slide 3

AlgoSec

Business-Driven Security Management

www.algosec.com

Categories

Security

Firewalls

Profile

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. Over 1,800 enterprises, including 20 of the Fortune 50, have utilized AlgoSec's solutions to make their organizations more agile, more secure and more compliant - all the time.

Solution at a Glance

AlgoSec is an automation solution for network security policy management that provides end-to-end visibility of the network security infrastructure, as well as business applications and their connectivity flows. With AlgoSec you can automate time-consuming security policy changes with zero-touch, proactively assess risk and ensure continuous compliance.

Use Case

State of Utah

State of Utah Network Security Management Breaks the Service Bottleneck. State government rapidly accelerates security policy changes while increasing security and compliance. For more information regarding State of Utah challenges and AlgoSec solutions Read Document. For more customer success stories click here

video

Return to Content
Slide 3

CGS Tower Networks

Enable and Optimize Cyber Security Solutions

www.cgstowernetworks.com

Categories

Cyber Security
Visibility
Packet Broker
Deduplication
Header Stripping
GRE Tunneling
Regex Filtering
Data Masking

Profile

In today's modern network architectures, cyber security and monitoring tools are challenged with data overload and lack of network visibility. The CGS packet broker solutions resolve these challenges by delivering the required network traffic in the right volume and in the correct format, resulting in improved service levels and significant reduction in cyber security risks.

Solution at a Glance

CGS is revolutionizing the packet broker industry by disaggregating packet broker hardware and software, allowing its customers to choose and benefit from a wide selection of modern, high quality mass production platforms that scale from the smallest to the most powerful packet broker in the industry, with the best performance and the most extensive feature sets.

Use Case

- Enable network visibility and minimize data overload
- Strip headers and achieve visibility into MPLS networks
- Adjust network rates to Cyber Security tools capacities
- Identify suspicious traffic using regex filtering and DPI
- Optimize BRO/SNORT deployments
- Extend Cyber Security solutions to remote sites
- Eliminate packet loss in case of network microbursts

video

Return to Content
Slide 3

ReSec Technologies

Zero Trust for Documents

www.resec.co

Categories

Network security

Email protection

Profile

ReSec Technologies is an innovative cybersecurity company, providing organizations with ultimate protection from file-based malware threats coming from email, removable devices, and file-transfer threat vectors (API, FTP, web downloads and uploads, file storage).

ReSec currently protects dozens of customers from diverse industries worldwide, including, finance, government, healthcare, telecommunications, oil and gas, military and defense and many more.

Solution at a Glance

ReSec's Content Disarm and Reconstruction (CDR) multi-engine platform treats every file as a threat and isolates it outside of the organization's network. ReSec then creates a new, threat-free, fully-functional replica of the original file and safely delivers it to the end user in real time. The result is a game-changing solution – a full-prevention gateway software that achieves unparalleled security against both known and unknown ("zero-day") malware, without compromising usability.

Use Case

ReSec has broad threat vector coverage. Common use cases are:

1. Email – protection from advanced threats, integration with O365, Gmail, and on-premise solutions.
2. File Portal – protection from external uploads into a digital portal.
3. API – protection from threats within documents, integration with any system via API.

video

Return to Content
Slide 3

CyberX

Battle-Tested Cybersecurity

www.cyberx.io

Categories

ICS/SCADA Cybersecurity, IoT Security

Profile

CyberX delivers the only IoT/ICS cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IoT and industrial control system (ICS) risk and preventing costly production outages, safety failures and environmental incidents, and loss of sensitive intellectual property.

Solution at a Glance

The CyberX platform combines patented, M2M-aware behavioral analytics and self-learning with proprietary threat intelligence to deliver immediate insights — less than an hour after being connected to the network — without relying on agents, rules or signatures, or specialized skills.

Use Case

The CyberX platform has been deployed in more than 1,800 production IoT/ICS networks to date, across all major geographic regions and industrial verticals.

Some notable customers include: 2 of the top 5 US energy utilities; a top 5 US chemical company; 2 top 5 pharmaceutical companies; a multi-billion dollar US consumer products manufacturer; a top 3 UK natural gas company; and national electric utilities across Europe and the Asia-Pacific region.

Return to Content
Slide 3

Radiflow

Industrial Cyber-Security Solutions for Critical Business Operations

www.radiflow.com

Categories

Cyber Security
OT Security
ICS/SCADA
Industry 4.0

Profile

Radiflow provides advanced cyber-security solutions & services to protect industrial networks. With the digital transformation of industrial facilities as part of the Industry 4.0, the asset owners are also facing new cyber security threats. Radiflow supports its customers throughout the cyber-security life-cycle to address these new challenges.With strong shareholders and an experienced leadership team, Radiflow solutions are deployed in x1000s of sites world-wide protection critical business operations.

Solution at a Glance

- A passive 3-tier industrial threat detection system with patented distributed smart-collectors feeding central traffic analytic servers.
- Ruggedized security gateways for policy enforcement.
- Risk assessment service using business impact for risk scoring and prioritization of mitigations.
- Managed services for OT SOC event analytics

Use Case

- Power Generation & Transmission & Distribution
- Renewable Power Plants
- Water & Wastewater facilities
- Oil & Gas
- Process Manufacturing
- Building Management Systems

Return to Content
Slide 3

SCADAfence

The Most Comprehensive **OT & IoT** Cyber Security Platform

https://www.scadafence.com/

Categories

Manufacturing

Critical Infrastructure

Building Management Systems (BMS)

Profile

SCADAfence, the global technology leader in OT & IoT cyber security, enables organizations with complex OT networks to embrace the benefits of industrial-IoT by reducing cyber-risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. SCADAfence protects some of the world's most complex OT networks, including the largest manufacturing facility in Europe.

Solution at a Glance

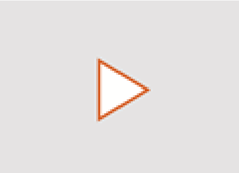
SCADAfence provides cyber security and visibility solutions for industrial ICS/SCADA networks in the manufacturing, critical infrastructure, and building management system sectors. SCADAfence secures industrial operations as they increase levels of production automation, IT/OT connectivity, and IIoT complexity. SCADAfence's passive solutions are designed to reduce the risks of operational downtime, product manipulation, proprietary data theft, governance and compliance, and ransomware attacks without affecting production environment availability.

Use Case

Vestel - Europe’s Largest Manufacturing Facility

Vestel’s OT network includes tens of thousands of devices that are divided into multiple production floors, and with dozens of switches on each production floor. To monitor the growing quantity of devices, sessions, connections, and bandwidth utilization in the network, a separate out-of-band monitoring network was set up to aggregate communications from the entire environment. Using the SCADAfence Platform and its ability to support large-scale throughput with best-in-class packet processing technology, SCADAfence was able to provide complete coverage for the entire facility - deploying only two appliances in two data centers.

video



Return to Content Slide 3

Cyabra

Solving Disinformation & Deepfakes (Fake News)

www.cyabra.com

Categories

Threat Intelligence

Media Analysis

Profile

Cyabra was founded 2 years ago, by a team of information warfare veterans from the IDF, with the purpose of exposing the truth in a post-truth era.

The company raised so far $3M, backed by a $8B Tier-1 VC (undisclosed), TAU Ventures and Alabaster.

Our customers include Warner Media, as well as the US State Department and the IL government.

Solution at a Glance

Our SaaS product filters out the fake from real, to make decisions based on unbiased & genuine opinions and content.

Use Case

- Election External Interference
- Election Internal Interference
- Detection of ongoing public opinion Influence
- Brand Health Analysis
- Corporate Intelligence

video

Return to Content
Slide 3

KELA

Targeted Cyber Intelligence

https://ke-la.com/

Categories

- Darknet
- Threat Intelligence

Profile

KELA was established in Tel Aviv, Israel in 2009. Offering a wide range of advanced proprietary technologies, KELA provides intelligence on threats targeting governmental agencies and corporate enterprises worldwide. KELA is comprised of more than 100 intelligence and technical experts all leveraging unique skills from Israel's elite military intelligence units. The combination of intelligence backgrounds and professionalism in the cyber world, enables KELA's team to develop high-end technologies and analyze complex data from an intelligence-point-of-view.

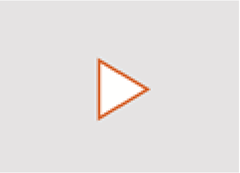
Solution at a Glance

KELA Group offers proprietary Darknet-based cyber intelligence solutions for enterprises and government agencies worldwide. KELA's automated technologies monitor a curated set of Darknet sources to alert clients of targeted threats. All threats are analyzed and qualified by KELA's analysts, ensuring all intelligence is 100% actionable.

Use Case

KELA's Cyber Intelligence Center uncovered the real identity of a threat actor dubbed SaNX – a handle that has become an infamous one among many security departments of numerous leading corporations worldwide. Throughout our research, we've also revealed his activities, his other handles in the Darknet, and affiliations he has to other hacking groups. The full story can be found on KELA's blog, here:

video



Return to Content Slide 3

Sixgill Ltd.

Deep, dark & beyond

www.cybersixgill.com

Categories

Artificial intelligence
Business intelligence
Machine learning
Information Security
Threat Intelligence
Natural Language Processing

Profile

Sixgill is a new breed of threat intelligence: Invisible. Proactive. Powerful. It is a fully automated cyber threat intelligence solution that helps organizations protect their critical assets, reduce fraud & data breaches & minimize attack surface. The platform empowers security teams with contextual, actionable insights with the ability to conduct real-time investigations. Rich data feeds such as *Darkfeed*™ harness Sixgill's unmatched intelligence collection capabilities & delivers real-time intel into organizations' existing security systems to help proactively block threats.

Solution at a Glance

A premium threat intelligence investigation platform: accurate, comprehensive, covert and automated. It proactively provides you with the insights you need to prevent data breaches, protect your brand, conduct investigations in real-time and minimize attack surface. Darkfeed complements the platform with rich data that supercharges your TIP, SIEM, SOAR & VM security platforms with unmatched, pre-emptive intelligence.

Use Case

1. Mitigating cybercrime and financial fraud risk to financial organizations. **2.** Alerting organizations that are being targeted by various cyber threats including malware, DDoS attacks, hacktivism campaigns and more. **3.** Assisting organizations protect their brand inter alia by alerting them of phishing attempts, rogue applications, pharming attacks and more.

4. Helping organizations better prioritize CVE patching using a state-of-the-art dynamic vulnerability rating.

Return to Content
Slide 3

L7 Defense

DISRUPTING THE WAY API'S ARE PROTECTED!

https://www.l7defense.com/

Categories

API Security:
WAF, DDoS and
BOT mitigation,
SAAS, cloud and
on-prem
Bring your own
licsence

Profile

L7 Defense ("L7") is an award-winning Israeli-based cyber security company. L7 developed its core solution named AmmuneTM that protects inline from the most sophisticated network, application and API level attacks with very high accuracy. By mimicking the human innate immune system activity, AmmuneTM identifies and mitigates attacks without the need for any external updates or active human intervention. The results are characterized by a low rate of miss-identification errors, which significantly outperform other solutions in this field.

Solution at a Glance

Ammune™ is a Revolutionary AI-Based Solution for API Security

Ammune™ API security platform, is an INLINE advanced Machine Learning solution that is made to actively protect APIs from the most advanced attack types, while hunting down "zero day" attacks with no impact on the normal traffic. Ammune™ API security platform discovers and defends automatically on each and every API. It iteratively builds negative and positive profiles of each API, that are used to spot and stop emerging threats that would otherwise go unnoticed. Ammune™ does not require previous experience of specific threats or pattern of activities.

Use Case

Discover | Automatic discovery of all web, mobile, and API-based connections, new & existing API's (with no agents)

Detect | Creates a unique management profile for customer's web, mobile, and API-based applications Business logic + Threat

Defend | Automatic Block, alert & report

Return to Content
Slide 3

NeuraLegion

Runtime Application Security Compliance On Every Build

www.neuralegion.com

Categories

Application Security Testing

Dynamic Application Security Testing

video

Profile

NeuraLegion is the first company providing a developer focused Dynamic Application Security Testing (DAST) solution enabling Runtime AppSec compliance on every build. Similar to the way Snyk & Fossa have revolutionized SCA and SonarQube & Semmle (Github) have transformed SAST by simplifying them and making them work for developers.

Solution at a Glance

We empower developers to incorporate our automated, 0-false positive DAST solution into every pull request so they can resolve security concerns as part of their agile development process. Our DAST platform integrates into the SDLC fully and seamlessly.

We can scan any target, whether Web Apps, APIs (REST & SOAP), Websockets or Mobile servers to help enhance DevSecOps and achieve regulatory compliance with our real-time actionable reports of vulnerabilities

Use Case

“We looked for a DAST solution that would provide us with broad detection capabilities which include restful and SOAP APIs and no other solution was able to meet these requirements. In addition integrating NexDAST into our SDLC was a breeze and we are able to detect and remediate vulnerabilities early while not wasting time trying to sift through false positives”

Vitaly Unic, Information Security Architect at Varonis

Success stories: https://go.neuralegion.com/resources

Reblaze

Web Application and API Security

www.reblaze.com

Categories

Web Application & Security

Cloud Security & Application

Profile

Reblaze provides cloud-based web security and protects against sophisticated attacks, exploits and other malicious activity targeted at your web assets. Reblaze incorporates the best intrusion detection mechanisms in a single, unified and integrated platform, which automatically protects your website from the moment it is connected to the service.

Solution at a Glance

Reblaze provides a NG-WAF, DoS and DDoS protection, Bot Management, API Security, scraping prevention, CDN, load balancing & more.

The platform offers a unique combination of benefits. Machine learning provides accurate, adaptive threat detection. Dedicated Virtual Private Clouds ensure maximum privacy. Top-tier infrastructure assures maximum performance. Fine-grained ACLs enable precise traffic regulation. An intuitive web-based management console provides real-time traffic control.

Use Case

The ideal Reblaze customer could be either a web based business, i.e., e-learning platforms. Or, one that his business heavily relies on web traffic, such as Medical centers (i.e., digital transfer of test results between doctors or medical institutions).

video

Reblaze

Web Application and API Security

Return to Content
Slide 3

Israel Cyber Security Catalog

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.