Accelerating U.S. - Israel

CYBER SECURITY COLLABORATIONS

Chicago | Boston | New York

September 8-12 | 2014

Welcome!

One of the greatest challenges facing us today is cyber security. We are all vulnerable to cyber attacks – whether it is in the public or private domain.

The threats are widespread and have led to such chronic problems as viruses, spam, spoofing, phishing and pharming, spyware, and key logging, just to name a few.

Cyber criminals are constantly improving their methods and are forcing industries and governments to do the same in order to protect themselves and stay ahead of the game.

The United States and Israel are more determined than ever to protect their businesses and citizens from these threats by introducing new legislation and policies. At the same time, they are also supporting the development of innovative cyber security solutions by companies in both countries boasting cutting edge high tech capabilities.

This year's delegation of leading Israeli cyber security companies is one example of such support and represents some of the best technologies that Israel has to offer.

We hope that joint development, business partnerships and investment opportunities will result from this week's activities.

> The Government of Israel Economic Mission to North America

> The Israel-U.S. Binational Industrial Research and Development Foundation (BIRD)

> The America-Israel Chamber of Commerce – Chicago

> The Consulate General of Israel to New England – Boston

> Matimop – The OCS' Americas Operations at MATIMOP

> The New England Israel Business Council

Accelerating U.S. - Israel Cyber Security Collaborations

Chicago, Boston & NY | September 8-12, 2014

Sunday, September 7, 2014 - Arrival in Chicago

Monday, September 8, 2014 - Chicago

9:00 am - 5:00 pm	On-site meetings with U.S. companies with selected Israeli companies *(Each Israeli company will receive its own itinerary)*
6:00 pm	Reception hosted by **Roey Gilad**, Consul General to the Midwest

Tuesday, September 9, 2014 - Chicago

8:30 am - 11:20 am	The 2014 Israeli Cyber Showcase Breakfast / Presentations / Networking and One-on-One Meetings KattenMuchinRosenmann LLP, 525 W. Monroe Street Keynote Speaker: Mr. **Brett Goldstein**, Chief Technology Officer, Grovesnor Capital Management and former CIO of the City of Chicago
11:30 am	Depart for O'Hare Airport

Tuesday, September 9, 2014 - Boston

6:30 pm	Reception hosted by **Yehuda Yaakov**, Consul General of Israel to New England, at his residence

Wednesday, September 10, 2014 - Boston

8:00 am - 10:30 am	Breakfast with investors

Agenda

Wednesday, September 10, 2014 - Boston

11:30 am - 2:30 pm	**"Cyber Security: Answering Tomorrow's Challenges"** A panel discussion featuring industry experts such as Akamai's Chief Security Officer, State Street's Chief Information Security Officer and Brigham and Women's Hospital's Information Security Officer The panel discussion will be followed by company elevator pitches and speed-dating
3:00 pm - 4:20 pm	Meeting with IT Directors of selected legal firms, hosted by **Mintz Levin LLP**
4:30 pm	Depart for Logan International Airport

Thursday, September 11, 2014 – NYC

8:00 am – 9:30 am	**Cyber Security Investor Breakfast** Israeli cyber security companies that are currently seeking investment will pitch to participating angel investors, VC's and private equity firms.
9:30 am – 2:00 pm	Israeli Cyber Security Showcase plus one-on-one meetings at **Goodwin Procter LLP** *(Each Israeli company will receive its own itinerary)*
2:30 pm – 4:00 pm	Roundtable of Hospital CIO's: • **Paul Shenenberger**, CIO, Summit Health Management • **John Sooley**, CIO, SUNY Downstate • **Ivan Durbak**, CIO, Bronx Lebanon Hospital • **Director of Information Security**, Atlantic Health System CIOs from several hospitals will speak with and present to the Israeli companies in a closed setting. Israeli companies will have the opportunity to learn about the hospital's needs and discuss with the CIOs about opportunities for collaboration.
6:00 pm – 9:00 pm	Dinner for the Cyber delegation organized with Stony Brook University at Abigail's Restaurant

Friday, September 12, 2014 – NYC

8:30 am – 2:00 pm	Grand opening of the National Security Institute (NSI) at **Stony Brook University** and meetings per requests

BIOCATCH

BioCatch - Cognitive Biometric Analysis

Company and Solution at a Glance
BioCatch Cognitive Biometrics Analysis transparently authenticates users in order to detect threats, reduce fraud and grow online business, while dramatically improving the user experience

Customer Challenges
How to reduce online fraud?
How to reduce friction with your online users?
How to add more functionality to your online sessions?
How to increase your end-user experience?

Offering
BioCatch offers a unique Online Fraud Detection technology that is able to authenticate, what was until recently considered, "high-risk" sessions

Unique Differentiators
BioCatch is the only online fraud detection vendor to leverage behavioral biometrics to authenticate online and mobile users. Using cognitive behavioral analysis, BioCatch creates a Cognitive Signature for each of the users, based on more than 400 parameters BioCatchcollects during a session. In addition, BioCatch leverages a unique patent pending technology that captures the responses to subtle Invisible Challenges™ introduced by BioCatch during the session.

Business Benefits for Clients
Less Friction
Less Fraud
More Functionality
More Security

References, Strategic Partners, Current Presence Outside Israel
Clients: Barclays, Zions, ING Direct, Itau, Microsoft, Sabadell
Partners: Many boutique partners that specialize in the security banking sector covering Latin America, Southern and Eastern Europe and AP
Investors: OurCrowd, Blumberg Capital

Contact: Avi Turgeman
Title: CTO & Founder
E-mail: avi@biocatch.com
Phone No.: +972-54-269-0895
www.biocatch.com

Covertix Ltd.

COVERTIX keep x safe

Covertix provides non-invasive file protection & control beyond the perimeters of the enterprise.

Company and Solution at a Glance
Covertix provides a cyber-security software solution for enterprise file control and data protection – anywhere. Covertix's patented SmartCipher technology is file type and platform agnostic and protects the greatest asset of any organization – its information, both inside and outside of the organization.

Customer Challenges
In today's data-driven world, confidential IP and regulated data is found within files. For the past decade, organizations have been spending a lot of money to secure their perimeter to protect them from external/ internal threats and regulatory violations. Once the files with confidential data leave the protected perimeter, the ability to control and protect sensitive data is lost.

Offering
Covertix's solutions enable internal and external parties to share confidential files while significantly reducing overall risk and with a minimal interruption to the organization's workflow.

Unique Differentiators
Covertix's technology tracks and monitors the usage of the protected files no matter where the files are located (internally and beyond the secured perimeter – no matter where the file goes or where it is stored). The technology is file and platform agnostic and does not require a change existing business driven behaviors.

Business Benefits for Clients
Covertix is able to monitor and protect any type of file, on any device (including mobile), with less integration effort from any other available technology and for a lower cost.

References, Strategic Partners, Current Presence outside Israel
History: Company was established in 2008
Clients: HMO, Banks, Financial Institutions, Legal Firms, Defense Bodies, Telecommunication Firms, Academic Institutions, Construction Firms
Partners: TecHarbor in Europe, ST Electronics in Singapore
Investors: Angel Investors
Customer Quote: Senior Vice President from a major Israeli bank: "Outside of Covertix, I haven't seen anyone else able to promise file security outside the bank."

Contact: Yoran Sirkis
Title: CEO
E-mail: ysirkis@covertix.com
Phone No.: +972-52-327-1101
www.covertix.com

Cybereason

Detect and Respond to Cyber Attacks in Real Time
Detect. Visualize. Terminate.

Company and Solution at a Glance
Cybereason developed a proprietary platform for detection and response to malicious hacking operations in real time. Cybereason provides security professionals with a full picture of each attack, minimizing false positives and enabling effective investigation, response and remediation.

Customer Challenges
In light of the magnitude and level of sophistication of recent cyber attacks, it is clear that attackers have the ability to penetrate corporate systems and remain undetected for long periods of time.

Most organizations may have hints of the malicious activities in their environments detected by various security solutions, but those are needles in haystacks, masked by the vast amount of false alerts.

There is a great need for a solution that can pick up only true evidence of attacks and build a meaningful story of the malicious operation in real time.

Offering
Cybereason's endpoint silent sensor continuously collects hints for known and unknown malicious activities within organizations. Then, Cybereason's behavioral analytics engine fuses the massive amounts of collected data, turning faint traces into a coherent picture of the malicious operation in real time. The gathered information is presented in a visual map of the malicious operation, providing security teams with actionable information about the attack and its context: timeline and propagation pace, affected endpoints, accounts, users and assets, involved malware, process, network traffic and more.

Unique Differentiators
- Receive full, actionable picture of a malicious attack: fusing faint hints into a coherent picture of the malicious operation.
- Context of the attack: receive information about the source of the attack, involved endpoints, assets, users, accounts, involved malware, propagation rate, network communication and more.
- Minimize false positive and enable fast incident validation

Business Benefits for Clients
- Reduce the time and effect of a breach
- Reduce time spent on false incidents
- Get actionable remediation steps

References, Strategic Partners, Current Presence outside Israel

History: Cybereason was founded in 2012 by elite members of the Israeli intelligence agency.
Clients: Cybereason is installed in a software services company in the US, a leading Israeli financial institution and an online media company in Israel.
Investors: Cybereason raised $4.6 million series A funding from Charles River Ventures (CRV).

Contact: Lior Div
Title: CEO
E-mail: lior@cybereason.com
Phone No.: 617-459-3651
www.cybereason.com

Fortscale

FORTSCALE
INTELLIGENT CYBER INSIGHT

Fortscale turns enterprise big data into User Intelligence

Company and Solution at a Glance
Fortscale's goal is to enable enterprise security analysts to easily run big data analytics for User Intelligence, regardless of their technical know-how.

Customer Challenges
Recent infamous security breaches are live examples of the growing challenges enterprises face from user related threats such as malicious insider threats as well as targeted attacks using hijacked user credentials.

Offering
Fortscale's solution provides User Intelligence to help discover and investigate suspicious behavior and generate leads about possible security breaches that are related to users' identity and behavior. Fortscale enhances SOC teams and security analysts' capabilities to that of advanced data scientists, while leveraging their existing infrastructure and know how. Fortscale's focus on an enterprise's users allows security teams to gain insights about malicious or rogue users, pinpoint high-risk user behavior and access activity.

Unique Differentiators
- User centric approach to combat security threats
- Sophisticated machine learning algorithms and analyst-friendly tool set interface

Business Benefits for Clients
- Discovers under the radar attacks and malicious insiders, to indicate a possible threat, with no pre-defined rules or heuristics.
- Maximizes client return from their security team and existing systems

References, Strategic Partners, Current Presence outside Israel
Fortscale was founded by seasoned security entrepreneurs, many of whom served in the IDF's Elite Intelligence and Cyber Unit, and is backed by Intel Capital and Blumberg Capital. Its team includes specialists in Big Data Analytics, Machine Learning algorithms and Cyber Warfare experts.

Clients: Product is installed in leading Global 2000 companies, including leading Fortune 100, from the financial, technology and retail segments.
Partners: Splunk is an official partner of Fortscale.

Contact: Idan Tendler
Title: CEO & Co-Founder
E-mail: idant@fortscale.com
Phone No.: +972-52-697-0215
www.fortscale.com

Lacoon Mobile Security

The Lacoon Mobile Threat Management Platform Can Detect, Assess and Mitigate Your Mobile Risks

Company and Solution at a Glance
Lacoon Mobile Security provides a mobile threat management platform that allows enterprises to easily manage and mitigate the risks of BYOD and protect corporate assets from mobile threats such as malicious applications, targeted attacks and Advanced Persistent Threats. Lacoon provides the most comprehensive solution for iOS and Android and it easily augments an enterprise's security and mobility infrastructure with real-time mobile security and intelligence. Its patented technology detects device, application and in-network threats that others miss and quantifies the risks and vulnerabilities that BYOD exposes to the enterprise.

Customer Challenges
- Proactive detection, prevention and mitigation of mobile threats
- Support for IOS and Android
- Non-intrusive user experience offering privacy protection and device performance preservation
- Minimize and manage the risk/exposure of employees mobile devices to corporate resources

Offering
Lacoon's unique multi-layer approach ensures enterprises have the visibility and coverage they need to manage their vulnerabilities and mitigate their risks. The Mobile Threat Platform delivers:
- Advanced Mobile Threat Detection
- Mobile Risk Mitigation
- Mobile Vulnerability Assessment

Unique Differentiators
Lacoon provides the most comprehensive solution for detecting advanced mobile threats, identifying vulnerabilities and mitigating the risk of BYOD. The solution is built for the Enterprise with integrations to SIEM, MDM, NAC, and IM that allow for rapid response to cross-platform APTs, broader visibility and more.

Technology advantages include:
- Advanced App Reputation
- Device and Network Anomaly Detection
- Adaptive Mitigation
- Dynamic Policy Enforcement

Business Benefits for Clients
With Lacoon, enterprises can balance the needs of mobile security and protection without impacting end user experience and privacy.

References, Strategic Partners, Current Presence outside Israel
Clients: Large Global Enterprise. Examples of customers include, Samsung, Intel, Zurich, Freshfields
Partners: Airwatch, Good, MobileIron, Samsung
Investors: Index Ventures

Contact: Michael Shaulov
Title: CEO
E-mail: Michael@lacoon.com
Phone No.: 415-589-9865
www.lacoon.com

Nativeflow

Nativeflow Enterprise Mobile Data Protection, Natively

Company and Solution at a Glance:
Nativeflow is a leading mobile data protection company. The Nativeflow solution provides a comprehensive, dynamically configurable mobile security solution for multiple enterprise security use cases: email security, mobile secure gateway, mobile attack protection and data leakage prevention.

Customer Challenges
With the shift to full connectivity via a plurality of devices, users are connecting to data via multiple mobile devices and multiple locations, leaving enterprise data at risk for tampering, malware and more. Nativeflow focuses on protecting the data so that users (employees, consultants, third party users and others) can access data with a native user experience while retaining user privacy.

Offering
A light touch, enterprise grade solution that focuses strictly on enterprise data, thereby allowing users to retain native user experience and user privacy, while allowing the enterprise to achieve full regulatory compliance.

Unique Differentiators
- Pinpointed protection on the corporate data
- Email Protection
- Data Leakage Prevention
- Enterprise App Protection
- Secure access to backend portals
- Compliance and regulation

Business Benefits for Clients
- Enterprise Grade Security
- Light touch solution
- Native user experience retained on enterprise owned and personally owned devices
- End-to-end security & auditing across aps, devices, users
- Organizations can retain compliance across all industries (HIPAA, Sarbanes Oxley etc.)

References, Strategic Partners, Current Presence outside Israel
Clients: Large insurance company (1000+ devices), large healthcare firm, large financial firm
Investors: JVP, OurCrowd

Customer Quotes / success stories:
"We evaluated many of the popular solutions for securing mobile devices but were not content

with the overall user experience. Nativeflow's solution offers us a transparent enterprise data protection solution that supports the many applications our users need to use to get their jobs done." CIO large insurance company

Contact: Tal Gilat
Title: CEO
E-mail: tal@nativeflow.com
Phone No.: +972-54-922-2476
www.nativeflow.com

RadiFlow

Secure your Distributed Utility Assets

Company and Solution at a Glance
RADiFlow provides secure communication solutions for critical infrastructure applications such as smart-grid, smart-city and oil & gas.

Customer Challenges
Critical operational assets (i.e. SCADA) are managed remotely over modern IP networks exposing them to cyber security threats without proper handling by the end-devices and the automation protocols.

Offering
RADiFlow provides a security IPS (Intrusion Prevention System) solution optimized for large-scale distributed automation applications. This solution is based on a service-aware firewall integrated into ruggedized access gateways, thus validating every SCADA command next to the automation devices.

Unique Differentiators
Our solution provides a security tool-set optimized for distributed SCADA applications unlike the classical security solutions for Enterprise/Internet applications.

The service-aware validation performed at each access point ensures that any abnormal activity in the internal SCADA network is detected and blocked.

Business Benefits for Clients
- Our integrated architecture enables an efficient deployment of SCADA security without an additional dedicated security layer in the network edges.
- This strict and yet cost-effective solution provides a very attractive risk mitigation cost-performance, addressing emerging regulations such as NERC CIP v5 and new insurance policies.

References, Strategic Partners, Current Presence outside Israel
RADiFlow was founded in 2009 as part of the RAD group and started commercial deployments by leading utilities world-wide in 2011.

RADiFlow solutions are distributed by local channel partners and global OEM vendors with the support of regional business-development offices in the US and UK.

Contact: Ilan Barda
Title: CEO
E-mail: Ilan_b@radiflow.com
Phone No.: +972-54-220-0960
www.radiflow.com

Safe-T

Safe-T allows organizations to unifiy all of their data exchange needs using a single simple and cost-effective platform while meeting regulatory requirements.

Company and Solution at a Glance
Safe-T is a provider of secure data exchange solutions for a wide range of industries, including financial, healthcare, and manufacturing organizations. Safe-T Box enables organizations to share data securely between people, applications, and businesses. It is designed for fast, easy deployment and wide user acceptance.

Customer Challenges
Allow organization to securely share data with customers and business partners, without changing the business users' day-to-day routines.

Offering
Safe-T Box, enables organizations to share data securely between people, applications and businesses and is designed for fast and easy deployment and wide user acceptance. Safe-T's RSAccess secure front-end solution eliminates the need to store sensitive data in the DMZ, thereby reducing exposure to data breaches.

Unique Differentiators
Organizations can conduct their business exchanging files securely without installing special software or setting up special accounts. Safe-T's Data Protection Suite can be deployed as Cloud, on-premise and hyrbrid deployments.

Business Benefits for Clients
- Streamline security into business processes
- Secure your enterprise data in transit and in rest
- Share data and emails securely from any device
- Achieve compliance faster, simpler and at lower costs
- Eliminate sensitive data from the DMZ while achieving ROI

References, Strategic Partners, Current Presence outside Israel
History: Safe-T Data was founded in 2013 by Amir Mizhar and Roei Haberman with $5M round A from a strategic investor in the cyber and homeland security space.
Partners: Safe-T partners with application and technology providers such as Sasa Software's Gate Scanner.

Contact: Eitan Bremler
Title: Director, Products & Marketing
E-mail: Eitan.Bremler@safe-t.com
Phone No.: +972-54-971-1007
www.safe-t.com

Seculert

Seculert Fills the Gaps in Enterprise Advanced Threat Protection

Company and Solution at a Glance
Seculert fills the gaps in existing advanced threat defenses by focusing on the blind spots found in breach prevention systems. In an era when infection is inevitable and adequate resources to find and remediate threats are limited, the Seculert platform identifies new threats with unprecedented speed and precision. Leveraging its Big Data analytics as a service, botnet interception, and elastic sandbox functionality, Seculert provides superior detection while driving down the cost and time it takes to remediate.

Customer Challenges
Having deployed modern prevention solutions and spent fortunes to recruit, hire, and train enough security specialists to operate; enterprises continue to be infected by the most malicious threats. Seculert addresses these issues by detecting and identifying infected devices and empowering security teams to isolate and mitigate new threats.

Offering
The Seculert's cloud-based platform uses a combination of botnet interception, log analysis, and elastic sandbox technology to detect new advanced threats as they appear on the network.

Unique Differentiators
The Seculert platform "sees" infected devices as they attempt to communicate with the command and control infrastructure operated by the perpetrators of modern cyber-threats. This requirement to "call home" is the point in the kill chain when cyber-threats are most vulnerable to detection and yet, is not adequately leveraged by many enterprises. The cloud-based Seculert platform also scales up and down as our clients needs dictate.

Business Benefits for Clients
- Improved security posture
- Faster time to remediation and value
- Enhanced SOC efficacy
- Reduced security headcount requirements

References, Strategic Partners, Current Presence outside Israel
History: Founded in 2010, Seculert has offices in the U.S., the U.K., and Israel.
Investors: Sequoia Capital, YL Ventures, and NVP

Customer Quotes / Success Stories: "Without installing anything, Seculert immediately provided a new level of advanced threat protection for all of our employees, including remote sites and users." Dor Liniado, Information Security Manager, ECI

Contact: John McCarty
Title: Regional VP
E-mail: John.mccarty@seculert.com
Phone No.: 484-994-4878

Contact: Dan Kunkel
Title: Regional VP
E-mail: Dan.kunkel@seculert.com
Phone No.: 630-740-8651

www.seculert.com

ThetaRay

"Protecting Your Critical Infrastructure Against Unknown Threats"

Company and Solution at a Glance
ThetaRay's solutions protect against unknown cyber, operational and fraudulent threats that target critical infrastructure and financial organizations. Leveraging patented Hyper-dimensional, Multi-domain Big Data Analytics™ developed by research groups in leading universities and validated by multiple organizations worldwide, ThetaRay's math-based, rule-free solutions are specifically designed to detect the unknown unknowns, in minutes rather than months, before any damage to critical networks or services can occur.

Customer Challenges
- Existing rule/signature/pattern-based solutions not capable of dealing with unknown threats
- Critical infrastructure and SCADA networks are becoming increasingly connected, thus, exposed

Offering
- Multiple solutions for the industrial and financial domains (cyber, operational, fraud)
- End-to-end threat detection including data processing, analytics and event investigation

Unique Differentiators
- Unmatched unknown threat detection
- Very low false positive rates
- Rule-free, real-time detection
- Continuous monitoring of thousands of parameters/dimensions from various domains
- Rapid threat mitigation leveraging laser-focused forensic information
- Fully automated detection

Business Benefits for Clients
- Prevent unplanned downtime - detect and take action before any impact to production, safety or revenues can occur
- Seamless integration - no changes to existing customer systems, critical networks or policies
- Same solution seamlessly protecting diverse environments
- Protect against external and internal threats
- Protect against future threats

References, Strategic Partners, Current Presence outside Israel
The company has generated massive interest in the industrial, financial and security industries gaining strategic investors, partners and customers such as General Electric and Citi Bank.

Contact: Udi Solomon
Title: VP Product
E-mail: udi.solomon@thetaray.com
Phone No.: +972-54-594-5720
www.thetaray.com

TopSpin

Defeating Attacks in Action

Company and Solution at a Glance
TopSpin's DECOYnet employs a powerful new approach for identifying advanced attackers that have bypassed current security solutions. It identifies threats, with 100% certainty, providing visibility of threat activities by luring attackers to an automatically-created "parallel network" (looks and feels exactly like the corporate network) while intercepting CnC traffic.

Customer Challenges
Current security measures - signature, sandboxing and anomaly detection solutions - get evaded by advanced attackers, provide only a limited view of the attackers' activities and require significant overhead for configuration and analysis. They are prone to false positives and attackers operate for months before being exposed.

Offering
DECOYnet identifies attacks at different phases. This gives a complete picture of activities and there is no hesitation when issuing an alert. It is composed of a balanced network of intelligent honey pots; set up automatically in the organization's environments, and sophisticated behavioral analysis of the organization's Internet traffic. DECOYnet's unique correlation of events from its different components into one actionable incident eliminates false alerts.

Unique Differentiators
- No false positives
- Complete picture and visibility of attacker activities
- Extremely high Threat Capture Rate
- Fully automated configuration
- Lures intruders away from the organization's assets and captures malware in a safe environment
- Listen-only mode minimizes exposure

Business Benefits for Clients
- Identifies compromised endpoints before data is stolen
- Protects sensitive data
- Detects insider threats
- Step-by-step forensic information
- Automation reduces the workload on the security team

References, Strategic Partners, Current Presence outside Israel
Installed in financial institutions and technology and infrastructure companies.

Contact: Doron Kolton
Title: CEO
E-mail: doron@topspinsec.com
Phone No.: +972-52-882-4865
www.topspin-security.com

Trustware

What happens in BufferZone,
stays in BufferZone

Company and Solution at a Glance
BufferZone defends endpoints against advanced malware and zero-day attacks with patented containment, bridging and intelligence technology. BufferZone maximizes user productivity with seamless, unrestricted internet access, while empowering IT with a simple, lightweight and cost-effective solution for isolating threats on up to thousands of endpoints.

Customer Challenges
Modern malware is designed to evade even the most advanced detection technologies, leaving endpoints vulnerable to attack. Since no form of detection can ever be correct 100% of the time, organizations need a new paradigm that contains potential threats while still enabling employees to make productive use of the internet, email and removable storage.

Offering
BufferZone's advanced endpoint security solution features:
- Container: Isolates browsers, email and removable storage in a secure, virtual environment to protect the endpoint and the network from threats
- Bridge: Securely transfers data from the container to the enterprise network to enable collaboration between people and systems
- Intelligence: Reports threat data from the container to enterprise analytics solutions

Unique Differentiators
BufferZone is the only solution that fully protects the endpoint while liberating the user. Unique features include:

- Support for removable storage as well as browsers, Email, Skype, Acrobat, Office and more
- Seamless deployment and management in a low-footprint, software-only solution
- Powerful and configurable bridge between the container and the organization

Business Benefits for Clients
- Maximize productivity with unrestricted internet access
- Defend endpoints against APTs, zero-day attacks and advanced malware
- Protect all windows devices both on-site and outside of the corporate network
- Deployment within hours, easy to manage through leading platforms
- Minimal resource utilization

References, Strategic Partners, Current Presence outside Israel

- Clients: Clal Insurance, National Insurance institute of Israel, Orbotech
- Investors: P Ventures, GND

Contact: Israel Levy
Title: CEO
E-mail: Israel.levy@trustware.com
Phone No.: +972-54-564-6030
www.trustware.com

VOTIRO

Protect your organization against tomorrow's threats

Company and Solution at a Glance
Votiro secures corporate data from cyber attacks rooted in unknown and zero-day exploits. Applied automatically to all files entering an organization, Votiro's patent-pending Anti-Exploit Technology neutralizes threats without having to detect them in advance. Votiro Spear-Phishing Protection eliminates threats in email attachments before they reach the mail server.

Votiro was founded in Israel by security experts experienced in safeguarding data in corporate, intelligence, and government organizations.

Customer Challenges
Unknown and undetectable by nature, zero-day threats enable attackers to enter organizations stealthily. When such exploits lie in genuine-looking ("spear phishing") emails, employees unknowingly compromise the entire organization merely by opening attachments. The challenge is to prevent known and unknown exploits from entering an organization, and to achieve this goal without disrupting business activity.

Offering
Votiro solutions automatically neutralize all incoming files—from email, removable media, and Internet downloads—before the files reach an organization's network. Votiro's unique Anti-Exploit Technology scans each file, makes microchanges (invisible to users) to its structure and metadata, and verifies compliance with the file format. These changes prevent malicious exploit code from dropping malware and spreading throughout the network. Easily deployable in the cloud or on premises, Votiro's solutions are mature and already employed by many customers.

Unique Differentiators
Standard cybersecurity methods cannot protect organizations from unknown or zero-day exploits. Votiro's technology provides unparalleled protection against such threats.

Business Benefits for Clients
- Safeguards intellectual property, business information, and customer data
- Protects against financial loss
- Preserves the organization's reputation
- Saves the cost of recovery
- Eliminates reliance on employees to reduce cyber risk

References, Strategic Partners, Current Presence outside Israel
Clients: Over 100 customers worldwide in banking, insurance, stock exchanges, government, security, telecom, energy, pharmaceuticals, and more

Partners: Local and international integrators; resellers; distributors
Customer Quotes / Success Stories: Provided on request

Contact: Itay Glick
Title: CEO
E-mail: itay@votiro.com
Phone No.: +972-73-737-4101/ 424-234-1424
www.votiro.com

White Cyber Knight

Business Visibility of Cyber Risk
Addressing the Supply Chain Resilience Challenge

Company and Solution at a Glance
WCK addresses Corporate America's "back door" vulnerability embodied in its unregulated small supply-chain (SMEs), which are a key hacker target. By combining portal-based online SME assessments, enforced cyber insurance and visual, business-driven intelligence, WCK fortifies the cyber resilience of America's large enterprises.

Customer Challenges
WCK addresses the "weakest link" of the small suppliers who comprise 42% of the source of the disruption at America's largest enterprises during cyber-attacks. These SME's are unregulated and completely neglected by the large assessment players (such as E&Y, Deloitte, Lockheed Martin, Boeing, etc.) due to their cost prohibitive assessment fees.

Offering
Leveraging its unmatched technology and risk analytics, WCK is offering a revolutionary, win-win business model for enhancing cyber resilience, at zero cost to the Enterprise, at almost zero cost to the supply-chain, while creating a new, huge cyber-insurance market of small companies who have undergone online assessments.

Unique Differentiators
We offer the only platform capable of handling the unique needs of risk assessments for Critical Infrastructures that include not only standard IT assets, but also operational technology and physical devices.

WCK's unique asset-framework shows how detailed cyber-risks affect critical business processes, in clear business language, without forgoing technical depth.

Business Benefits for Clients
We overcome the built-in financial challenges of supply-chain cyber resilience for both large organizations, as well as the small supply-chain by offering superior assessment capabilities and automation, at almost zero cost, while creating for ourselves a huge revenue opportunity based on the cloud model.

References, Strategic Partners, Current Presence outside Israel
Sample Clients: Royal Mail, GDF Suez, BASF, Teva Pharmaceuticals, Amdocs, UBI Bank, MasterCard
Partners: McAfee, Gray Matter Systems, Atos, Devoteam, and others

Customer Quotes / Success Stories: ***"We see WCK as a game changer. I can finally centrally control and report intelligently to the CIO and CFO..."*** Ilan Abadi, CISO of Teva Pharmaceutical Industries (NASDAQ: TEVA).

Contact: Eyal Adar
Title: CEO & Founder
E-mail: eyal@wck-grc.com
Phone No.: +972-54-440-0028

Contact: David Furstenberg
Title: COO
E-mail: df@wck-grc.com
Phone No.: 914-331-1048

www.wck-grc.com

Government of Israel
Economic Mission to North America

Foreign Trade Administration
MINISTRY OF ECONOMY

The Government of Israel Economic Mission to North America Foreign Trade Administration, Ministry of Economy

The Israel Economic Mission facilitates collaboration, trade and investment between Israel and North America, and operates five offices in the U.S. and two in Canada. We are part of the Foreign Trade Administration at the Israeli Ministry of Economy, which is responsible for managing and directing the international trade policy of the State of Israel.

We serve as a gateway for American companies that would like to explore investment opportunities in Israel and for Israeli companies looking to develop and expand their operations in the U.S.

Our mission provides guidance and business opportunities for companies interested in raising capital, exporting goods and services, and finding technological or strategic partners. We also provide information on available grants, loans and incentives that the Israeli government provides to foreign investors.

Year-round, we support hundreds of companies and arrange dozens of Israel-related conferences, business delegations and investment events around the world, but especially in the United States and Israel. We work with every sector of the economy, including high tech, new media, consumer goods, life sciences, cleantech, food and wine.

Contact us for more information. We look forward to hearing from you.

Chicago

Mr. Yariv Becher
Consul, Head of Economic Mission
Israel Economic Mission to the Midwest
111 East Wacker Drive, Suite 1230
Chicago, IL 60601
Tel: 312-332-2160
E-mail: Yariv.Becher@israeltrade.gov.il
www.itrade.gov.il/us-chicago

New York

Ms. Nili Shalev
Economic Minister to North America
Israel Economic Mission to the East Coast
800 Second Avenue, 16th Floor
New York, NY 10017
Tel: 212-499-5610
E-mail: Nili.Shalev@israeltrade.gov.il
www.itrade.gov.il/us-ny

BIRD

BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation

Israel - U.S. Binational Industrial Research and Development Foundation (BIRD)

BIRD is a key catalyst for joint Research & Development between U.S. and Israeli companies, focusing on emerging industries and novel technologies with significant commercial potential.

BIRD Partnerships
Any pair of companies, one Israeli and one American, may jointly apply for BIRD support so long as they have the combined capability and infrastructure to define, develop, manufacture, market, sell and support innovative products based on industrial R&D.

Risk-Sharing Enhances Cooperation
The BIRD Foundation offers conditional grants for joint development projects on a risk-sharing basis. The Foundation funds up to 50% of each company's R&D expenses associated with the joint project. Repayments are due only if commercial revenues are generated as a direct result of the project. If a project fails, BIRD claims no repayments.

BIRD acquires no equity in the companies supported and no intellectual property rights in their products. The foundation does not interfere in formulating or managing the relationship between the partnering companies.

For additional information, please refer to our website **www.birdf.com**

In Israel

Eitan Yudilevich, Ph.D.
Executive Director
Tel: +972-3-698-8300
E-mail: eitan@birdf.com

Ms. Limor Nakar-Vincent
Director, U.S. Business Development & BIRD Energy
Tel: +972-3-698-8315
E-mail: limorn@birdf.com

In the U.S.

Ms. Michal Miasnik
West Coast Representative
Tel: 650-752-6485
E-mail: michalm@birdf.com

Ms. Andrea Yonah
East Coast Representative
Tel: 609-356-0305
E-mail: andreay@birdf.com

NEIBC

Driving Collaboration and Promoting Innovation between Israel and New England

The New England Israel Business Council (NEIBC) is a nonprofit, member based organization dedicated to increasing economic development opportunities in Israel and New England by connecting people and businesses, supporting investment opportunities and promoting vibrant collaborative business community which will produce long term sustainable growth. NEIBC provides a diverse program of activities and events and offers advice in doing business in these two regions.

The NEIBC supports this collaboration. Our goals are to:

Connect: meet and collaborate with a tightly connected network of professionals committed to mutual goals.

Support: Encourage investment opportunities in both regions through public and private sector partnership.

Promote: Advance the innovative and unparalleled economies of Israel and New England and the strong partnerships that exists between the two.

Produce: Create new initiatives and partnerships between the two regions which lead to long term economic development opportunities.

Contact us for more information. We look forward to hearing from you.

Ms. Adi Golani
Executive Director
155 Seaport Boulevard, 15th Floor (at Foley Hoag)
Boston, MA 02210
Tel: 617-633-2342
E-mail: adi@neibc.org
www.neibc.org

The OCS' Americas Operations at MATIMOP

MATIMOP מתימו"פ
מרכז התעשייה הישראלית למחקר ופיתוח
Israeli Industry Center For R&D

The Office of the Chief Scientist (OCS) MATIMOP's Americas Operations was established in 2013 with the objective to expand Israel's research and innovation collaborations in the Americas. As part of its mission, it creates high impact partnerships and operates funding programs for industrial R&D and innovation with US States (including CA, NY, MA, MD, MI, FL, SC, OH, VI and more). These platforms provide funding, risk sharing and facilitate market entry to the US and global markets.

These programs provide the US companies and research partners access to Federal and State funding sources. Israeli companies participating in these programs can apply and **receive OCS grants** for joint projects with US partners. In particular, through these programs, the **OCS KIDMA Program** funds Israeli companies taking part in bilateral projects with US partners. MATIMOP helps in **partner matching** and **scouting** of relevant technology providers for joint projects in any field.

Among OCS/ MATIMOP's North American Partners are the National Cyber security Center of Excellence (NCCoE), Massachusetts Clean Energy Center, Massachusetts Technology Collaborative, Massachusetts Life Sciences Center, Space Florida, SCRA – South Carolina, The Center for Nanoscale Science and Engineering (SCNSE) in New York, the Center for Excellence in Wireless and Information Technology (CEWIT) in New York, Advanced Energy Research and Technology Center (AERTC) in New York, Michigan Economic Development Corporation, California Office of Economic and Business Development, Development Services Agency (Ohio), Technology Development Corporation Maryland, Maryland Department of Business and Economic Development, Colorado-Israel R&D Program, Wisconsin-Israel R&D Program, Virginia-Israel R&D Program, Oregon-Israel R&D Program, The National Research Council (NRC) of Canada, Natural Resources Canada (NRCan), International Science and Technology Partnerships Canada (ISTPCanada), Agriculture and Agri-Food Canada (AAFC), The Ministry of Economic Development and Innovation (MEDI), Government of Ontario, The Health Technology Exchange (htx.ca) and The Ontario Brain Institute (OBI).

INTERESTED IN APPLYING BUT DON'T HAVE A PARTNER?
MATIMOP offers free of charge assistance in identifying a US or Israeli partner for a joint project.

If you wish to submit a bilateral project with a US or Israeli partner, or a partner scouting request, please contact:

Ms. Liron Eldar
US-Israel Industrial R&D Programs Director
E-mail: liron@matimop.org.il
Tel: +972-3-511-8155
www.matimop.org.il/usa.html

America-Israel Chamber of Commerce Chicago (AICC)

The America-Israel Chamber of Commerce Chicago (AICC) provides an opportunity-laden venue for companies to do business in Israel, as well as between members. The AICC organizes informational, networking and state-of-the-art business programs, promotes Israeli goods and services, leads trade delegations, and works closely with governmental, non-profit, charitable and industry organizations to foster trade and investment.

Members include manufacturers, distributors, wholesalers, retailers, professional and business service providers, venture capitalists, investment bankers and R&D scientists. Over the years, hundreds of companies have found ways to grow their international trade through the Chamber.

WE:

- Facilitate trade and investment between the US and Israel
- Promote Israeli goods and services
- Present business networking and educational programs
- Lead trade delegations and business match-making events
- Work closely with the Government of Israel to advance bilateral trade

Contact us for more information. We look forward to hearing from you.

Mr. Michael Schmitt
Executive Director
203 N. LaSalle St., Ste. 2100
Chicago, IL 60601
Tel: 312-558-1346
E-mail: m.schmitt@americaisrael.org
www.americaisrael.org

Consulate General of Israel to New England

Israel, very much like New England, is ideally positioned to become a global cyber hub thanks to a unique combination of academia, industry and government. The Consulate General of Israel to New England aims to promote the Israel cyber industry and explore potential collaboration with New England's relevant businesses, academic institutions, and government entities via a series of events, conferences and networks.

The Consulate's Department of Innovation and Economic Affairs is responsible for increasing and advancing economic development and commercial partnership between New England and the State of Israel. Our office works closely with the financial community, venture capital funds, leading international companies and top research institutes, thus enabling us to establish platforms for productive business and technology collaboration throughout New England.

We provide a wide range of services, with special expertise in the cyber security industry:

- Funding and investment opportunities
- Global expansion
- Operational support
- Co-marketing activities

Contact us for more information. We look forward to hearing from you.

Mr. Baruch Nudelman Perl
Director of Special Projects
20 Park Plaza
Boston, MA 02116
E-mail: cons.gen.assistant@boston.mfa.gov.il
Tel: 617-535-0208 **Fax**: 617-535-0255
http://boston.mfa.gov.il

Acknowledgments and Special Thanks

to all the people and organizations that supported the program

> In Chicago:

Mr. **Ari Rokni**, Director of Business Development, Government of Israel Economic Mission to the Midwest
Mr. **Michael Schmitt**, Executive Director, America Israel Chamber of Commerce Chicago
Mr. **Dan Sabel**, President, America Israel Chamber of Commerce Chicago
Ms. **Debra Rade**, President, Rade Law
Mr. **Jan Hertzberg**, Director of Technology Risk Services, Baker Tilly Virchow Krause, LLP
Mr. **Brian Rosenzweig**, Managing Partner and Chief Marketing Officer, JANVEST

To our hosts:
Mr. **Leonard Ferber**, Partner and co-head of Technology practice, Katten Muchin Rosenman LLP
Mr. **Roey Gilad**, Consul General of Israel to the Midwest, for hosting the delegation in his residence

> In Boston:

Mr. **Jonathan Shapira**, Goodwin Procter LLP
Mr. **Bill Schnoor**, Partner, Goodwin Procter LLP
Mr. **Yaniv Kapluto**, Mycroft, Inc.
Mr. **Baruch Nudelman** Perl, Associate Director of Special Projects, Consulate General of Israel to New England

To our hosts:
Goodwin Procter LLP
Mr. **Yehuda Yaakov**, Consul General of Israel to the New England, for hosting the delegation in his residence

> In New York:

To the Israeli Economic Mission's team:
Mr. **Oded Grinstein**, Deputy Economic Minister
Mr. **Erik Blumberg**, Director of Investment Relations
Mr. **Josh Berliner**, Director of Social Media
Ms. **Rebecca Weinberg**, Director of Cleantech
Ms. **Beth Belkin**, Director Media and PR
Ms. **Fay Cleveland**, Administrative support

Ms. **Andrea Yonah**, East Coast Representative, BIRD Foundation

To our hosts:
Goodwin Procter LLP
Stony Brook University, Department of Computer Science

> In Israel:

Mr. **Avi Shavit**, OCS and Ms. **Liron Eldar**, Matimop, for assisting in recruitment of the Israeli companies; Ms. **Maha Wakileh** and Ms. **Chava Doukhan**, BIRD Foundation, for designing and editing the booklet and marketing information, Ms. **Einat Spivak**, BIRD Foundation, for general support and company coordination

A special thanks to: Mr. **Yariv Becher**, Israel Economic Mission, Chicago, Ms. **Nili Shalev**, Israel Economic Mission, New York, Ms. **Adi Golani**, New England Israel Business Council, and Ms. **Limor Nakar-Vincent**, BIRD Foundation, for leading the program of the Cyber Security delegation and related events.

MATIMOP מתימו"פ
מרכז התעשיה הישראלית למחקר ופיתוח
Israeli Industry Center For R&D

MATIMOP: Israeli Industry Center for R&D
www.matimop.org.il/usa.html

America - Israel Chamber of Commerce
Chicago

Israel Economic Mission to the Midwest
www.americaisrael.org

BIRD
Israel-U.S.
Binational Industrial Research and Development Foundation

Israel- U.S. Binational Industrial research and Development Foundation
www.birdf.com

Government of Israel
Economic Mission to North America

Israel Economic Mission to the East Coast
www.itrade.gov.il/us-ny
www.itrade.gov.il/us-chicago

NEIBC

NEIBC -The New England Israel Business Council
www.neibc.org

Consulate General of Israel to New England

Consulate General of Israel to New England
http://boston.mfa.gov.il