










Israel's Leading IT Security Companies






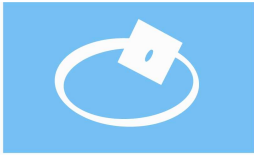


המכון הישראלי לייצוא ולשיתוף פעולה בין-לאומי
The Israel Export & International Cooperation Institute



Company Name	Website	Brief Description	Technology
<p>Actimize</p> 	<p>www.actimize.com</p>	<p>Actimize is a leading provider of enterprise software solutions for anti-money laundering, brokerage compliance, and fraud prevention. Actimize solutions enable financial institutions to increase their insight into real-time customer behavior and improve risk and compliance+ performance.</p>	<p>Built on a single, shared risk platform, Actimize solutions allow clients to consolidate financial crime monitoring and case management activities across the organization. Fraud Prevention - A complete set of solutions to detect and prevent fraud enterprise-wide. Actimize's remote banking, ATM/Debit Card, wire and ACH payments, deposit and employee fraud solutions have been proven in benchmarks against other leading vendors to detect more fraud with fewer false positives. Anti-Money Laundering - Integrated capabilities to support customer due diligence, watch list/sanctions filtering, and suspicious activity and transaction monitoring. Solutions that monitor virtually every banking product have been proven in deployments in dozens of countries at card issuers, regional and global banks, building societies and other financial institutions. Enterprise Risk Management - A comprehensive case management platform that unifies a bank's financial crime and information security needs to ingest, aggregate, investigate and manage cases and issues across the entire organization. Benefits include centralized SAR filing, workflow enforcement and a true holistic customer view.</p>
<p>ActivePath</p> 	<p>www.activepath.com</p>	<p>ActivePath is developing innovative software solutions for secure e-mail communications targeted to the financial industry, governments and service providers. ActivePath provides e-mail security protection, allowing organizations to safely and confidentially conduct business over the Internet. ActivePath is offering bi-directional bank to customer communications over email.</p>	<p>All the solutions in the ActivePath product line provide protection against viruses and attacks, and enable policy-based message filtering, encryption and signatures.</p>
<p>AGS Encryptions</p> 	<p>www.agsencryptions.com</p>	<p>AGS Encryptions is an innovative security and software company, packing leading-edge security acumen, advanced technology solutions, software development, R&D track record and vast Internet experience. AGS has developed ultra fast cryptography, unique storage value device, digital coins, bank-less transaction platform, with groundbreaking e-payment, m-payment and instant reward redemption applications.</p>	<p>Cryptography</p>
<p>Beyond Security</p>	<p>www.beyondsecurity.com</p>	<p>Beyond Security specializes in developing tools that uncover security holes in servers, expose vulnerabilities in the corporate network, check computer systems for the</p>	<p>Beyond Security utilized the knowledge accumulated in SecuriTeam to develop the Automated Scanning engine. Automated Scanning performs a security mapping of the</p>




		<p>possibility of hostile external attacks and audit vendor products for security holes. The company developed an innovative vulnerability assessment platform called Automated Scanning that automatically performs security assessment services and Managed Security Services (MSS) on periodic basis using advanced vulnerability scanning technology.</p>	<p>organization's network and simulates attacks originating from either the internal or the external network. Once the security mapping is complete, Automated Scanning generates a detailed vulnerability report specifying the security breaches, along with several practical and easy-to-apply solutions to fix those vulnerabilities. The engine is updated on a regular basis for the most recent security vulnerabilities. The updates include security vulnerabilities that were discovered by the company's research and development team, as well as those discovered elsewhere.</p>
<p>CallingID</p> 	<p>www.callingid.com</p>	<p>CallingID's technology protects consumers from phishing, fraud, identity-theft and being a target of spam attacks. Use of CallingID's technology uniquely creates a focus on only accessing reputable sites by identifying site ownership and ratings to the user before these sites are actually accessed from their browsers, emails and instant messages. It also provides real-time alerts when personal data is about to be entered on a form. CallingID offers a way to immediately add the following required features to Consumer Security software vendors: Safe Browsing, Site Reputation Rating, Privacy Protection, Anti-Phishing, Anti-Malware, Spam Avoidance, and Anti-Spyware. CallingID offers both Toolbar and Link Advisor Software packages and a software development kit (SDK). Both Toolbar and Link Advisor provide multi-language support.</p>	<p>CallingID has developed a rich set of technologies and several extensive knowledge bases enabling us to ensure user safety by the implementation of the following: - Real time anti-phishing: When a user logs into his web account he knows that this is really the site he intended to reach - it is not a phishing site. - Trojan and spyware bypass technology that evades Trojans such as key-loggers. When a site has signed as CallingID Safety Seal Verified, even if the user's machine is infected by a Trojan, the password typed by the user cannot be detected. - A unique database of web site owners and a technology for automatic identification of the owner of any web site. CallingID applies a unique knowledge base, multiple technologies and databases. - Automatic detection of more than 50 different errors in web sites and web pages. - Automatic detection of man in the middle and DNS spoofing attacks.</p>
<p>Checkmarx</p> 	<p>www.checkmarx.com</p>	<p>Checkmarx develops and markets automatic enterprise software suite to detect security vulnerabilities in the software source code. Its main product enables organizations to meet new policy security and business software compliance, and reduce correction time and overall development cost by finding vulnerabilities in the software application during the Software Development Lifecycle before they reach QA or production.</p>	<p>Checkmarx' CxSuite automatically detects technical as well as business logic security vulnerabilities in the source code during and after the Software Development Life Cycle (SDLC). At first, the software analyzes the source code to establish its "DNA", by mapping static characteristics such as interrelations and dependencies, and then it computes the data dynamic flows. This data mapping is then fed into Checkmarx' Query Engine, which in turn parses query commands concerning the source code and returns its results. Checkmarx unique data mapping is optimized to allow unprecedented flexibility in querying the code, with unmatched accuracy and speed. The software includes an extensive knowledgebase of all the types of attacks and the conditions that would allow these attacks to take place. The knowledgebase exists as a set of high-level queries to the Query</p>



			Engine and is available for every stage of the development. By tracking all possibilities of attacks, the software provides precise risk assessments and suggests the best remedies.
<p>ClearBIT Systems</p> 	www.clearbit.com	ClearBIT Systems, a digital currency solutions startup, is developing its patent-pending prepaid stored value transaction platform, pioneering a new form of currency designed for the digital age -random bits. The ClearBIT Platform offers loyalty program, electronic commerce and mobile commerce corporations a cost efficient, bank independent and mathematically secure alternative to credit card platforms and ATM networks.	ClearBIT Systems' patent-pending technology consists of a random bit secured, prepaid stored value transaction platform and unique stored value devices. The combined e-payment infrastructure is the first-ever bank independent, non-account-based, mathematically secure and 100% anonymous, digital currency transaction system.
<p>Commtouch Software</p>  <p>Real Security. In Real Time.</p>	www.commtouch.com	Commtouch® provides proven messaging and Web security technology to more than 100 security companies and service providers for integration into their solutions. Commtouch's patented Recurrent Pattern Detection™ (RPD™) and GlobalView™ technologies are founded on a unique cloud-based approach, and work together in a comprehensive feedback loop to protect effectively in all languages and formats. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures and enabling safe, compliant browsing.	Commtouch Recurrent Pattern Detection™ and GlobalView™ technologies analyze vast amounts of data from the Internet backbone in real time, to enable secure, compliant email communication and web browsing. The solutions are content- and language-agnostic, so are equally effective in all parts of the world, including spam and web pages in Asian languages. The offerings are in the form of engines, daemons, or software development kits (SDK), which security vendors or service providers integrate as one element within their own offerings as an OEM technology.
<p>Covertix</p> 	www.covertix.com	Covertix's innovative technology enables organizations to track, monitor and control documents and files anytime, anywhere, within and outside of the organization. The system utilizes an innovative concept which transfers the file protection responsibility to the file itself, each file encapsulates a dynamic set of rules which defines the appropriate protection, and thus the file becomes a "self-protecting file". The protection can be transparent to the end-user, occurring automatically based on centrally managed business rules taking into account document content, source, location or usage. The protection schema can be modified and updated by the system at any given time.	Covertix has a unique and innovative approach to solving the problem of Information Leakage. The company's patent pending self-protecting file protects itself anytime, anywhere. Any file can be protected, without changing the original document and usage. Protection is user driven or automatic, appropriate security policy enforces access and usage rights of the information the file holds. It doesn't matter if the file is lost, stolen or moved from its secure place. The file always knows what actions are allowed and by whom. In addition, the file can track, monitor and log its usage and report to "central command" providing organizations for the first time with the ability to asses their high-level information exposure. Furthermore, Organizations can dynamically change the policy and prevent and control access to files even when it is out of the organization! The process is transparent to end users and is done covertly.



	www.cyber-ark.com	<p>Cyber-Ark is an Information Security company that develops and markets digital vaults for securing and managing sensitive information within and across global enterprise networks. Based on its patented Vaulting Technology(TM), Cyber-Ark's digital vault products include: Inter-Business Vault(R), a secure infrastructure for cross-enterprise data exchange of highly-sensitive information; Sensitive Document Vault(TM), for secure storage and management of highly-sensitive documents, and Enterprise Password Vault(TM), for the secure management of administrative, emergency and privileged user passwords. Cyber-Ark's Vaulting platform has been tested by ICSA Labs, an independent division of Cybertrust.</p>	<p>Cyber-Ark's approach is much like that of a physical vault at a bank. We create an electronic vault, or safe haven, in the network. Regardless of the overall network or security surrounding it, the safe haven is extremely secure. At the same time, Cyber-Ark's unique approach makes this information more accessible—eliminating the traditional tradeoff between accessibility and security. In addition, the Vault provides multiple security layers that are traditional and well known such as VPN, file access control, encryption, authentication and a firewall. Cyber-Ark also provides Visual, Manual (dual control), and Geographical security to round out the layers. Each layer is highly integrated with other layers and has intimate knowledge of the other making the implementation proprietary. The layers themselves do not, by design, interact with other systems - increasing the overall security of a Vault.</p>
	www.easy2comply.com	<p>Dynasec's mission is to provide a platform that enables organizations to efficiently manage risk, governance and compliancy processes. The company developed Securitive™, a suite of web-based applications that enables companies to continuously manage and control compliancy, corporate governance and risk management processes. Securitive™ offers a common repository that enables companies to manage many regulations in one system.</p>	<p>Information Security Management Software (ISMS).</p>
	www.enforcive.com	<p>Enforcive provides compliance and security software products for IBM Power i (AS/400) and mainframe server platforms of IBM as well as related open server platforms. It offers a combination of access management, monitoring, auditing, reporting, IDS alerting and general security management.</p>	<p>Data security & compliance. Enforcive's security and auditing products are suitable for IBM System i, IBM System z (mainframe), Microsoft Windows and SQL Server, Unix and Linux platforms. The company's latest product, the Enforcive Cross Platform Audit, provides Security Event Management for companies using IBM Power i and/or IBM mainframes as their mission critical servers. Through the Cross Platform Audit, companies can correlate IBM mainframe, IBM Power i, Windows, AIX, Linux, SQL Server and DB events through online logs as well as advanced reporting & dashboards.</p>
<p>GED-I</p>	www.ged-i.com	<p>GED-I develops and markets unique security to storage devices, SAN, NAS, DAS and Tape, utilizing multi layered security, encryption, proprietary structuring and interference to recovery tools. Thus, GED-I offers security</p>	<p>GED-i's unique security technology specifically designed with regard to the special characteristics of today's storage devices in mind. Storage data security based on plain encryption is not satisfactory due to storage device's inherent vulnerabilities:</p>

		<p>to storage data that overcomes the inherent vulnerabilities of the storage devices. The company's products include verity of security appliance (GSA 2000) for Enterprises and SMB and Encryption Key Server (GKS 2000).</p>	<p>known data structure, huge volume of data, data recovery technologies and the retractable storage disks. The GED-i Ltd product family GSA 2000, is the only solution that guarantees that your stored data will never be compromised by unauthorized organization or individual. Encryption solutions can be implemented by a Superior or IBM Integrated Superior configuration, based on combination of one or more GSA 2000-EE (Encryption Engines) connected to a single GKS 2000 (Key Server) or using an All In One configuration, utilizing single unit of GSA 2000-AIO.</p>
<p>HexaLock</p>  <p>HEXALOCK</p>	<p>www.hexalock.com</p>	<p>HexaLock is a technology-based company that develops and markets digital copy protection solutions that help prevent unauthorized copying of digital content, when stored on optical or other digital media.</p>	<p>Based on a powerful and unique architecture HexaLock technology offers publishers a new level of available digital copy protection. HexaLock is committed to go beyond the standard and visible technologies in order to offer the most powerful, comprehensive and easy-to-use copy-protection solutions</p>
<p>Hybrid Application Security</p> 	<p>www.hybridsec.com</p>	<p>Hybrid Application Security is engaged in creating the 3rd generation of application security. Using artificial intelligence, Hybrid Telepath detects 0-day attacks on web applications and back-end business logic. Hybrid's solutions provide a holistic approach to web fraud prevention by implementing real-time detection and tracking technologies arming the website owners with higher resolution of view into their online business activities.</p>	<p>Enterprise security solutions to mitigate fraudulent and malicious web application user actions.</p>
<p>mConfirm</p> 	<p>www.mconfirm.com</p>	<p>mConfirm is a leading developer of fraud prevention solutions for credit and debit cards. mConfirm's focus is on location-based solutions aimed at combating point of sale (POS) and ATM fraud. Using a combination of patent-pending technologies and advanced algorithms, mConfirm's solutions analyze credit card transactions in real time to prevent fraud and reduce false alert rates, helping card issuers save millions of dollars in fraud losses and risk management costs. mConfirm's innovative solutions can operate both as a stand-alone system and as a complementary performance-enhancer for existing systems.</p>	<p>mConfirm is committed to protecting payment card issuers from fraudulent use of cards. Combining two unique methodologies, mConfirm offers an advanced authentication method and location-based analysis (LBA) processes, to detect and prevent fraudulent transactions. The authentication method is implemented based on the cellular authentication concept, which relies on the cellular carriers' location-based services (LBS)(See "Authentication concept"). The location-based analysis (LBA) functionality (See "Location Based Analysis") incorporates a vast set of patent-pending algorithms and analysis procedures that converge into a powerful, real-time, fraud detection tool. The LBA does not rely on cellular location-based services. The</p>

			authentication and LBA solutions are highly effective when combined; each solution enhancing the other's learning capabilities and overall performance. Confirm's solutions are very effective as a stand-alone system, but can also successfully enhance existing systems to maximize the customer's total investment in fraud detection solutions.
 <p>Profitect PROFITECT turn losses into profits</p>	www.profitect.com	Profitect's profit-amplification solution enables you to quickly discover and actualize untapped profit opportunities across the entire retail value chain. Profitect's algorithms quickly identify measurable profit optimization opportunities through the identification of value chain margin leakage, shrink, waste, process errors, and operational risks and damages - returning intelligent, prioritized actions for increasing profit.	The Profitect Suite is a modular solution that can be quickly deployed in your enterprise environment, sitting on top of existing systems. With easily integrated data from POS, ERP and core systems, the deployment can happen in a matter of weeks. In addition, the solution require minimal time commitment of IT resources for implementation and maintenance. With an intuitive user interface, training and support requirements are also kept to a minimum, allowing your organization to amplify profits quickly and with minor disruption to standard operating procedures.
 <p>Safend safend Securing Your Endpoints</p>	www.safend.com	Safend a leading provider of endpoint data protection, guards against corporate data loss and theft through its content discovery and inspection, encryption and comprehensive device and port control. Safend encrypts internal hard drives, removable storage and CD/DVDs and provides granular port and device control over all physical and wireless ports. Safends maps sensitive information and controls data flow through email, Web, external devices and additional channels. Safend ensures compliance with HIPAA, PCI, SOX, BASEL II and other regulatory data security and privacy standards. Safend solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe.	The key to the success of Safend's innovative endpoint security solutions is the underlying Digital Membrane technology. With the understanding that every endpoint has a different set of external interfaces, based on differing standards but all leveraging the standard IP protocol stack - Safend created a protocol-level, generic, semi-permeable barrier that can be "wrapped around" any device. At the heart of this barrier - dubbed "Digital Membrane" - is a unique kernel-level protocol inspection engine that analyses in real time all inbound and outbound communication interfaces for a given device. The engine examines all seven protocol layers - from the physical to the application layer. The Digital Membrane monitors and controls all incoming and outgoing traffic for each device - blocking or allowing access or data based on highly-granular security policies. Barrier permeability is controlled in accordance with organizational security policy – granularly defined in the Safend Security Management console. The result - total policy-based monitoring and control at all protocol layers – enabling previously unheard-of visibility and control over devices, applications, and actual data transferred.
Seculert	www.seculert.com	Seculert helps corporations, governments and service providers detect cyber threats without the need for time-consuming and costly network integration efforts. The	Data Security, Cloud Computing, SaaS. Seculert has developed breakthrough, patent-pending technology that provides early detection of a broad array of cyber threats affecting an

		<p>company has developed an innovative, patent-pending technology that provides early detection of a broad array of cyber threats affecting its customers' networks. Powered by this technology, Seculert's cloud-based Cyber Threat Management complements and strengthens enterprises' existing security infrastructure, enabling fast and cost-effective deployment without the need for new hardware, software or any changes to the corporate network.</p>	<p>enterprise's network. Utilizing this technology, our "in the cloud" Security-as-a-Service complements and strengthens enterprises' existing security infrastructure, enabling fast and cost-effective deployment without the need for new hardware, software or any changes to the corporate network.</p>
<p>Secure Islands Technologies</p> 	<p>www.secureislands.com</p>	<p>Secure Islands Technologies Ltd. provides the most advanced information protection and control (IPC) solution incorporating innovative, intelligent data-centric security technology. Secure Islands' objective is to redefine the way enterprises secure their information assets. Secure Islands provides an effective method to secure enterprise sensitive information anywhere – through central governance. This is accomplished by embedding encryption and policy into the information itself while eliminating the need to secure the channels or the mediums.</p>	<p>Secure Islands has built a next-generation information protection and control (IPC) solution, which addresses the challenge fundamentally different from any other IPC or data loss prevention (DLP) solution currently available in the market. This solution contains several innovative technologies – enabling organizations to uniquely identify sensitive information, control it and protect it, while reducing maintenance efforts and with no affect on user productivity. Nexus Data Identifier™ is a patent pending data identification technology that classifies the data in the transition point (Nexus Point) in which the data transfers from its structured form to its unstructured form. Nexus Data Enforcer™ is a patent pending data enforcement technology that enforces protection into the data in the transition point (Nexus Point) in which the data transfers from its structured form to its unstructured form – providing an integrated solution that addresses the three different aspects of IPC – data at rest, data in motion, and data in use. IQP Architecture is based on agents to server design which is applicable to various IT environments. In addition, the protection engine which is responsible to apply the enforcement is based on industry's most proven third party E-DRM and encryption products such as Microsoft AD RMS.</p>
<p>SecuSystem</p> 	<p>www.secu-system.co.il</p>	<p>SecuSystem develops, produces and markets the machine-readable SecuSystem technology for counterfeit protection, widely considered the most sophisticated technology suitable for widespread use against counterfeiting and related fraud.</p>	<p>SecuSystem consists of two parts - a unique security ink printed on the document or on the label or packaging of the product to be protected, and an optical reader for authentication. The presence or absence of the security feature on the protected item is determined by the use of a reader or authenticator. There are two basic categories of readers, small, portable, handheld readers which provide authentication signals to their operator OEM readers incorporated into and communicating directly with</p>

			<p>larger data processing systems. SECUSYSTEM customizes its security products to meet customer needs, while providing anti-counterfeiting features with SecuSystem technology. Authentication of a SecuSystem requires that a match be obtained between the feature's signature, as measured by the reader, and the vision of an authentic signature which is stored in the reader's memory.</p>
<p>SentryCom</p> 	<p>www.sentry-com.net</p>	<p>SentryCom provides proactive solution for ID fraud, that "bad guys" will not be able to circumvent. Traditional IT security means like Anti-Virus or other defenses - fail to prevent from malware to infest our computers. Competitive products fail to operate in infested environment, are inconvenient to use and too costly. Our novel Malware-Resilient Strong Authentication and Crypto Software provides viable and convenient protection for mission-critical data and online transactions.</p>	<p>SentryCom's technology is incorporated in the MACS – Managed Authentication and Crypto Software, delivered as Private or Public SaaS (Software as a Service.) Our Offering: Secures transaction and ensures user's identity; Scalable to enable medium to high risk transactions; No need to call-back customers to verify transaction; No need for costly hardware tokens or software certificates; Seamless integration into existing transaction flow; User convenience and self-serving administration; Complies with Advanced Electronic Signature; Simple integration with Web-site; Un-structured data files protection independent of infrastructure; Applicable across the board from enterprise servers to laptops to USB drives to email to cloud storage.</p>
<p>Versafe</p> 	<p>www.versafe-login.com</p>	<p>Versafe is a private and independent security applications development house. The company's products are a direct result of years of consulting services provided to leading financial organizations, hands on security work and some of the best talent and experience in the online security field. With time, Versafe's line of products has grown to contain software and supporting services, with an active operation center, backing up the company's operations around the clock. The Versafe security suite provides a comprehensive, real-time solution covering the full range of identity theft methods employed by attackers: Phishing, Trojan and Pharming. Its state-of-the-art, proprietary, online Anti-Fraud solution and technology enable organizations of all sizes to mitigate the risks of identity theft and take control over the protection of their clients' sensitive credentials and online information.</p>	<p>Versafe Anti Trojans Technology - Using layered security, automatic engines and a 24/7 operation center, Versafe efficiently detects computers infected with Trojans, attempting to gain access to the organization's servers. Advanced encryption of user log-in credentials, eliminates the risk of the Trojan, key logger or session hijacker. Versafe Anti Phishing Technology - Using layered security, automatic engines and a 24/7 operation center, Versafe efficiently detects phishing attacks as they are being set up, monitors the fraudulent activity, documents the incident and takes down the fake site, all before scam e-mails are sent to the organization's customers. The collected information then serves for forensic investigation of the event and for laying the ground to protect against the next wave of attack. Anti-Pharming - Pharming is a dangerous attack that includes MITM (Man in The Middle), DNS poisoning and others, which is difficult to detect. In recent years, it has become more and more prevalent, affecting a growing number of organizations around the world. By implementing the Versafe Anti-Pharming online</p>

			mechanism, which detects different types of Pharming attacks, it is possible to identify servers that execute MITM attacks, and also to identify the users targeted by these attacks, in real time. The use of these protective components allows preventing connection from a public network in which Pharming attacks are carried out, including ARP poisoning, DNS poisoning and others.
<p>White Cyber Knight (WCK)</p> 	<p>www.whitecyberknight.com</p>	<p>White Cyber Knight (WCK) provides managers with a better understanding and more effective management skills for their GRC (Governance, Risk and Compliance) status. WCK's methodology relies on a patent pending approach - EESA© (End-to-End Security Assessment). EESA© is a realization of our vast global experience in the security and IT risk fields. White Cyber Knight's solutions are used by large and medium enterprises. We help organizations with the important task of understanding their GRC situation, and guide them to transfer that understanding between management and technical staff. In recent years, IT systems have grown in complexity and volume. Few IT or business managers today have a clear overview of their organization's IT-GRC status, or their related risks on a real-time basis.</p>	<p>WhiteCyberKnight is a comprehensive Risk Management platform designed for large organizations. It provides all Risk Management practitioners expert tools risk management, risk analysis and managerial Security Risk Dashboard. The tool is based on an advanced RA engine. It is capable of providing a comprehensive Risk Map, that is driven by a wide variety of aspects, affecting organizations security. This includes: human behavior, policies and regulations, architecture of IT systems, and technical vulnerabilities, among others. The tool it designed to meet RM needs in large organizations, but can effectively be used by medium-sized organizations as well. It provides the ability to manage security risks in distributed environments and allows the Chief Security Officer (CSO) and the IT manager to measure their success. For Customer Case Study - Multinational Bank press here.</p>
<p>WonderNet</p> 	<p>www.penflow.com</p>	<p>WonderNet was founded as a joint project between Wacom of Japan and Graphitech of Israel, which specializes in the artistic CAD/CAM market. WonderNet is a biometric signature authentication company offering the Penflow solution. The system is based on inherent proprietary patents that validate a signature in a quick, non-invasive and highly accurate manner. The Penflow(TM) authentication engine views the signing process as a series of movements performed in a continuous, consistent and sequential process.</p>	<p>WonderNet has developed a new and unique algorithm that allows signature authentication by monitoring human hand movements instead of the final image. The authentication is performed employing parameters such as pen speed, acceleration pressure and directional vectors. The proprietary algorithm enables the signature profile (not its image) to be matched automatically. The algorithm contains learning elements so that all the natural changes in a signature are continuously updated into the learning profile that is on an average, less than 1KB. Penflow(TM) technology is mature and proven. Penflow(TM) requires no special computer knowledge or training, and is "as simple to apply as signing your name". An off-the-shelf product, Penflow(TM) is endorsed by financial, military, industrial and legal institutions. Dynamic signature verification replaces or complements a personal identification number, passwords, hardware devices such as cards (magnetic or SIM) or keys as a means for identity verification.</p>

