

SPECIAL STUDY

The Changing Landscape of IT Security: Emerging Trends and the Role of Israeli Innovation

Dan Yachin

IDC OPINION

The IT security industry is undergoing fundamental changes, driven by issues such as information-intensive regulations, the blurring in the traditional distinction between insiders and outsiders, and the increasing usage of consumer applications and unmanaged mobile devices in corporate environments, to name a few. The move is toward a focus on protecting the information itself, rather than merely the perimeter, against an ever-growing list of potential threats. IDC believes that the following trends will reshape the IT security industry in the coming years:

- ☒ Information-centric security technologies and solutions are emerging in parallel with the commoditization of other security functionalities. In accordance, emerging security fields focused primarily on protecting sensitive information and business processes – including data loss prevention (DLP), secure collaboration, governance, risk management, and compliance (GRC) – are gaining attention.
- ☒ The growing convergence of security, systems, storage, and network management, as well as increasing use of managed security service providers (MSSP), represent a mind shift toward reducing operational complexities while consolidating and outsourcing a wider range of common security functionalities that are more network-focused and perimeter-centric.
- ☒ To a large extent, this global trend is fueled by innovative start-up companies, which have emerged in recent years to offer various related solutions. Many of these companies originate in Israel, which has served historically as a center of innovation for the global IT security industry, as in the cases of firewall and network security, encryption, and others. Looking at the current activities of Israeli security start-up companies can help shed some light on the future of IT security.

TABLE OF CONTENTS

	P
IN THIS STUDY	1
SITUATION OVERVIEW	1
Introduction: The Shifting Focus of IT Security	1
Emerging IT Security Trends	1
Information-Centric Security	1
Convergence of Security, Systems, Storage, and Network Management	2
Web Security	3
GRC	3
Managed Security Services	3
The Israeli IT Security Industry: A Global Center of Innovation	4
Background	4
The Check Point Driver	5
Israel IT Security Industry Overview	5
Main Fields of Activity	8
Essential Guidance	13
Learn More	13
Related Research	13

LIST OF TABLES

	P
1 Recent Acquisitions of Israeli IT Security Companies	7
2 Notable Israeli IT Security Companies	9

IN THIS STUDY

This study discusses major trends in the global IT security industry, as well as the evolving market needs and solutions that will drive the next generation of IT security. It also provides a historic overview of the Israeli IT security industry as a global center of innovation and explains how Israeli companies are addressing emerging market trends.

SITUATION OVERVIEW

Introduction: The Shifting Focus of IT Security

For nearly two decades, organizations have been focusing their IT security efforts on protection from external threats posed by growing exposure to the Internet. In deploying an expanding array of solutions – firewalls, antivirus, antispam, intrusion detection/prevention, anti-spyware, and others – most organizations have built solid walls to protect their perimeters.

Today, for various reasons, many of them are realizing that, while perimeter security remains an important need, protecting sensitive information – patents, trademarks, brands, trade secrets, designs, architectures, copyrights, algorithms, software code, hardware schematics, inventions, business processes, and many other corporate assets – should be the top security priority.

The driving force behind this concern is the potential impact of failing to safeguard those assets. The risks of inadvertent or deliberate disclosure of confidential information and intellectual property range from legal culpability to competitive disadvantage. Companies risk major financial losses when design documents and source codes are posted on Internet message boards or emailed outside of their organizations. A privacy failure, even merely a perceived failure to protect customer data, can result in the loss of consumer trust, affect customer retention, and cause significant damage to a brand and to company reputation.

At the same time, various trends are heralding a change in the way organizations are managing some of the main components of their security environments. For the most part, these trends relate to simplifying the management of ongoing security operations through convergence of functionalities, outsourcing various security solutions, and automating management processes, among others. The combination of these is gradually driving a move from a network-focused and perimeter-centric stance toward embracing environments that are data-focused and information-centric.

Emerging IT Security Trends

Information-Centric Security

The growing number of high-profile incidents in which customer records, confidential information, and intellectual property have been leaked (or lost/stolen) has created an explosive demand for solutions that protect companies from the deliberate or inadvertent release of sensitive information.

Moreover, numerous information-intensive government and industry regulations are requiring organizations to protect the integrity of customers' and employees' personal information and corporate digital assets.

IDC believes that information protection and control (IPC) solutions will play key roles in protecting sensitive information and helping companies to comply with privacy regulations. Addressing IPC issues is a complex challenge. The increasing use of corporate email, Web email, instant messaging (IM), peer to peer (P2P), and other channels for distributing data and the proliferation of mobile devices that enable employees to carry sensitive information outside of an organization's boundaries make the control of information a substantial challenge. IDC believes that IPC solutions are evolving to discover, protect, and control information contained in data in motion, data at rest, and data in use to help organizations of all sizes and from all industries to achieve the following:

- ☒ To comply with government and industry regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act, and European Union Data Protection Directive
- ☒ To prevent violations of corporate policy and best practices
- ☒ To stop the loss of intellectual property and proprietary information
- ☒ To prevent high-profile leaks of private information and customer records and
- ☒ To preserve corporate brand image and reputation

The IPC concept represents a major change in mindset among organizations regarding IT security. However, it becomes increasingly apparent that in order to effectively protect sensitive information, a perimeter-centric IPC approach is becoming less and less effective due to the growing complexity of IT environments and the need to apply protection on the multiple conduits through which sensitive data may be leaked.

Alternatively, some emerging IPC solutions are based on embedding security into the data itself, rather than detecting and preventing unauthorized delivery at the exit points (e.g., through email and Web channels, USB drives, and mobile storage devices). This channel-agnostic approach can be used to protect information during its entire lifecycle – through creation, distribution, and storage.

Convergence of Security, Systems, Storage, and Network Management

IDC coined the term 3S to represent the convergence of storage, security, and system management. 3S companies are responding to customer complaints about the increasing difficulty and complexity of administration, which is exacerbated by multiple management stovepipes.

3S has grown out of the realization that security is something that is critical to business success. Security will increasingly require a cross-disciplinary approach that manages many business aspects and not just isolated issues such as network access and antivirus. It must look at what individuals are doing and how data is created, stored, processed, and destroyed. It is a driving need for 3S vendors to provide the capabilities to offer data protection throughout its lifecycle, as mentioned above.

Web Security

A growing number of malicious codes are exploiting weaknesses in protocols (e.g., HTTP, POP3, FTP, and HTTPS) and Internet browsers, and infected Web pages are becoming a more prominent way to exploit a site visitor's computer remotely, without the visitor even having to physically click on any links or email attachments. The number of Web sites distributing malware has increased explosively, as malware creators continue to extend their distribution channels. As a result, Web security is a growing concern for organizations, and IDC believes that Web-based attacks will continue to become more malicious and sophisticated. Web-security solutions will thus play an increasingly important role in ensuring security.

IDC also expects hackers to target the growing number of Web 2.0 sites, which are extremely vulnerable in this regard. Hackers will leverage the popularity of Web 2.0 to target the greatest number of Internet users. The practice of hackers planting malicious code on legitimate Web sites is rampant. Hackers' utilization of popular Web sites to install malicious code and steal confidential (personal or business) information is increasingly widespread. It will no longer be sufficient to block access to only those inappropriate Web sites that often contain malicious code. Web security vendors must also deal with detecting malware on legitimate Web sites.

Web 2.0 also presents a significant data-loss-prevention challenge for many enterprises. Message boards, blogs, and social networking sites are becoming pipelines for information leakage and corporate compliance violations. A recent IDC survey showed that some 37% of confidential information leaks occurred via the Web. The same survey also showed that around 67% of organizations expressed monitoring employees' use of the Web to prevent data leaks and compliance violations to be a major consideration. Given that Web 2.0 exposes organizations to both inbound and outbound security threats, IDC believes future Web security solutions must analyze traffic bi-directionally.

GRC

Historically, IT governance, IT compliance, and IT risk management existed as discrete functional silos within corporations. Developments in global regulatory and legal environments are compelling many corporations to take a unified approach. As compliance and risk management regimes are growing in complexity and because efforts have been slow to realize the projected savings from their ongoing IT compliance efforts, corporations are seeing a need for enhanced visibility into and accountability for the effectiveness of their compliance and risk management efforts.

Managed Security Services

The threat landscape, in which complex and sophisticated attacks are now a means of financial gain, has evolved along with technology. Organizations need a secure and cost-effective way to manage their networks, systems, and applications, as well as their information assets, while staying focused on their primary fields of business. In addition, security processes require both constant review and policy enforcement, given the volume and severity of external threats such as viruses, spam, and denial of service, not to mention internal threats, including data leakage and new emerging vulnerabilities from the deployment of new technologies. Furthermore, a lack of in-house security expertise, together with the cost of security experts, makes it very challenging for a company to set up and manage a security system. Both the managed security services market and the hosted security services market thus

represent tremendous opportunities for service providers, as customers are looking for cost-effective means of managing and monitoring their security infrastructures.

In a given enterprise, it will not be a choice between on-premises (software/appliance) and off-premises (hosted security service) deployments. Rather IDC predicts enterprise environments will embrace a hybrid approach that leverages the email hygiene benefits of an in-the-cloud hosted service with the granular policy enforcement and data-loss-prevention benefits of an on-premises software or appliance solution. Systems integrators, telcos, and security vendors will participate in this new generation of managed services.

The Israeli IT Security Industry: A Global Center of Innovation

Background

Today, the Israeli IT security industry is an entire ecosystem that consists of multiple established vendors and small start-up companies, service providers, and other players operating in various IT security-related technology fields. The vast knowledge and experience gained by these companies is the primary driving force of this industry, supporting its evolution and the continuous creation of new technologies and solutions, as well as new companies providing them.

The establishment of the local IT security ecosystem was enabled by a number of factors and circumstances. In fact, the proliferation of this industry is strongly aligned with the success of the entire local high-tech industry, which has a reputation for being one of the largest centers of technology innovation in the world. This success has been driven by government support, a strong academic research infrastructure, the creation of an entire ecosystem surrounding and fueling the high-tech industry, and a healthy entrepreneurial spirit in Israel, among others.

The significant growth of the Israeli high-tech industry began in the early 1990s, with significant investments in resources and infrastructures by the Israeli government. Among these efforts, two major initiatives played a significant role in establishing Israel as one of the main global hotbeds for technology innovation and entrepreneurship – the Technologies Incubator project and the Yozma project.

The Technologies Incubator project was aimed at establishing a framework for thousands of scientists and engineers to develop technological solutions, while meeting all of the financial, infrastructural, and technological needs of these individuals in this early stage. This initiative served as one of the main drivers for the establishment of the Israeli start-up industry. In addition, during the early 1990s, the Israeli government supported the establishment of several government-owned venture capital (VC) funds through the Yozma Group, which provided the foundation for the local VC industry. Since that point, both local and top-tier foreign VC firms have made significant investments in thousands of technology start-up companies, making Israel one of the largest centers of start-up activity.

Innovation and entrepreneurship in IT security has been greatly driven by intensive research and development (R&D) efforts in the areas of network and data security undertaken by the Israel Defense Forces (IDF) intelligence and communications units. The unique needs of these units have fueled the development of new ideas and technologies. The exposure to these developments and the practical experience gained have inspired many Israeli IT security entrepreneurs to develop various

innovative commercial technologies, such as the firewall technology, which was developed by the Check Point Software Technologies founders, who served in an elite IDF intelligence unit.

In addition, many technologies and solutions developed by Israeli IT security companies are related to local academic research in this field, especially in the area of encryption. The single most significant example is the research of Dr. Adi Shamir of the Weizmann Institute of Science, who co-developed the RSA encryption algorithm in 1977, which uses a private and public key pair for authentication. Most encryption engines available on the market today are based on this algorithm.

The Check Point Driver

Over the years, Israeli IT security vendors have established themselves as leading players in their domains. Some of them leveraged their positions to become publicly traded companies. Historical examples include Memco, a provider of distributed client/server systems for internal security, which went public on NASDAQ in 1996; in 1999, Platinum Technology acquired it for more than \$500 million. A more recent example is Aladdin Knowledge Systems, a leading provider of authentication and network security solutions publicly traded on NASDAQ since 1993, which was acquired by Vector Capital in January 2009 for \$160 million.

Israel's most important and long-lasting success story in the IT security space is Check Point Software Technologies, which was founded in 1993 and went public on NASDAQ in 1996. The company innovated network security when it developed a statewide inspection firewall and improved the technology's ease of use with policy management firewall tools based on a graphical user interface (GUI). The company employs approximately 1,800 people. Today, it is among the leading network threat management solutions vendors, and its products are sold, integrated, and serviced by a network of 2,200 distributors, OEMs, resellers, managed service providers (MSPs), and partners in 88 countries. It serves corporations, service providers, small and medium-sized businesses, consumers, and more than 85 telecommunications and Internet service providers worldwide. The company's customer base includes all of the Fortune 100 companies and nearly all (98%) of the Fortune 500 companies, as well as tens of thousands of businesses and organizations of all sizes.

Check Point Software Technologies is consistently one of the leading Israeli IT companies in terms of revenue and market capitalization. Beyond that, the company made a significant contribution to the continuous proliferation of the Israeli IT security industry by educating and providing key practical experience for thousands of employees. Additionally, a significant number of ex-Check Point Software Technologies executives and employees have left the company to launch their own start-ups, helping establishing Israel as one of the major global centers of IT security innovation.

Israel IT Security Industry Overview

The abovementioned drivers laid the foundation for the establishment of the Israeli IT security industry. As a result, since the mid 1990s, the number of Israeli IT security companies has grown significantly. Joined with new security needs due to the growing popularity of the Internet, the local IT industry began establishing its position as a global center of innovation.

Over the years, Israeli companies have been responsible for the development of some of the most innovative and groundbreaking security technologies and have

become worldwide leaders in their domains. Israeli IT security companies were pioneers in various technology fields, such as firewall and network security, Web application security, authentication, encryption, DLP, Web security, and anti-fraud.

In accordance, most leading global security vendors have established local R&D centers, in most cases following acquisitions of Israeli IT security companies (see Table 1). As a result, many of their major product lines are being developed in Israel. These include companies such as CA, Cisco, Microsoft, McAfee, Websense, and EMC (RSA).

Successful acquisitions and IPOs made by notable Israeli IT security start-ups have made this sector one of the main investment areas for both local and foreign VCs. Since 2004, companies in this field have raised more than \$1 billion in funding.

TABLE 1

Recent Acquisitions of Israeli IT Security Companies

Date	Company	Acquirer	Deal Value (US\$M)	Field
Jan 09	Aladdin Knowledge Systems	Vector Capital	160.00	Authentication, network security
Nov 08	Eurekify	CA	30.00	Identity and access management
Oct 08	IDFocus	CA	N/A	Identity and access management
Jan 08	FraudSciences	Paypal	169.00	Anti-fraud
Jan 07	Secured Dimensions	Microsoft	5.00	Application security
Dec 06	PortAuthority	Websense	90.00	Data leak prevention
Oct 06	Onigma	McAfee	20.00	Data leak prevention
May 06	Whale Communications	Microsoft	76.00	SSL VPN
Feb 06	Snapcentric	VeriSign	12.00	Anti-fraud
Dec 05	Cyota	RSA	145.00	Anti-fraud
Nov 05	V-Secure	Radware	15	Intrusion prevention
Aug 05	KaVaDo	Protegrity	N/A	Web application security
May 05	Puresight	Boston Communications	5.80	Web content filtering
Jul 04	Sanctum	Watchfire	45.00	Web application security
Jun 04	Magnifire	F5 Network	29.00	Web application security
Mar 04	Riverhead	Cisco	39.00	Network security

Source: IDC, 2009

Main Fields of Activity

Today, there are about 150 active Israeli IT security companies operating in a wide range of fields, which closely reflect the abovementioned global trends. For example, a relatively large number of Israeli companies are providing various types of solutions as a managed service (also referred to as 'security in the cloud'), including network security, endpoint security, and GRC. Other examples include companies that are offering combined platforms for system, network, and security management catering to the 3S trend and emerging providers of centralized frameworks for managing multiple GRC functionalities.

Looking into current primary fields of activity, it appears that the Israeli IT security industry remains highly focused on its traditional strengths and areas of expertise, such as encryption, network security, and anti-fraud, but it is also expanding into new domains. A growing number of network security players are expanding into Web security, while a number of specialized players are offering various dedicated solutions to address related threats and concerns.

In some cases, Israeli companies are pioneering new technological approaches in the IPC space, and this has been one of the main areas of activity for Israeli IT security companies that have traditionally specialized in encryption technologies. In addition, Israeli companies have been among the earliest entrants into the emerging DLP market – Safend, PortAuthority, and Onigma (the latter two acquired by Websense and McAfee, respectively), among others.

At present, the trend in this space is toward information-centric security, and Israeli companies are active in heralding this new field – from established players such as Check Point Software Technologies, which has recognized this field as a main strategic direction, to start-up companies that are bringing innovative approaches and solutions to addressing emerging IPC challenges.

TABLE 2**Notable Israeli IT Security Companies**

Company	Field	Description
Aladdin	Authentication, network security	Aladdin Knowledge Systems provides software digital rights management (DRM), USB-based authentication, and enterprise secure content management solutions. The company's products include the HASP family of software DRM products, which is designed to provide software developers and publishers with software protection, licensing, and distribution solutions; eToken USB-based authentication; and eSafe secure Web gateway.
Algosec	Network security	Firewall operations and security risk management solutions for managing complex dynamic firewall, router, and VPN environments.
Altor Networks	Network security	Monitoring and firewall software solutions for auditing inter-VM traffic, enforcing security policies, and gaining visibility and control over virtual network traffic.
Applicure	Web security	Web application security solutions that protect Web sites and Web applications from external and internal attacks.
APPprotect	Digital content protection	Designed for software companies, APPprotect provides anti-piracy protection solutions that are based on splitting the software binary code into two parts, one part resides on the user's machine and the other on secure servers located across the Internet.
ARX	Digital content protection	Digital signature solutions that allow users to electronically sign documents, forms, and messages within major applications such as MS-Word, Adobe-Acrobat, ERP, and Content Management systems.
Beyond Security	GRC	Vulnerability management solutions that detect security holes in servers, expose vulnerabilities in the corporate network, check computer systems for the possibility of hostile external attacks, and audit vendor products for security holes.
Bio-Guard	Biometrics	Biometric identification management solutions that integrate palm vein authentication, facial recognition, fingerprint identification, and voice recognition.
Breach Security	Network security	Web application security solutions that protect organizations against Internet hacking, as well as identity theft, information leakage, and insecurely coded applications.
Bsafe	Network security	Network and data security products for IBM iSeries (AS/400), zSeries (mainframe), and open systems.
C.D.I. Systems	Digital content protection	ePublishing solutions that combine DRM with Web content management and other tools, allowing organizations to protect intellectual property and sensitive information that is placed on the Internet.
Check Point	Network security, IPC, mobile security, Web security	Check Point provides a range of security software and hardware products and services, including UTM solutions, firewall/VPN appliances, intrusion prevention products, remote access solutions, endpoint products, management platforms, and other standalone security products – in areas such as Web security, consumer security, and mobile security. While Check Point has primarily been offering perimeter gateway security solutions, over the past few years the company has moved to providing a fully integrated architecture for perimeter, internal, Web, and endpoint security. To support this expansion, Check Point has made several acquisitions in recent years, including Zone Labs, NFR, Protect Data, and the recently acquired Nokia's security appliance line.
Checkmarx	Source code analysis	Secure source code solutions that automatically detect technical and business logic vulnerabilities in the source code across the software development life cycle.
CommTouch	Network security	Cloud-based messaging and Web security solutions that automatically analyze Internet traffic in real-time to identify new spam, malware, and zombie outbreaks as they are initiated.
Confidela	IPC	Software as a service solutions for document security and control.
ControlGuard	IPC	Endpoint security solutions that protect, manage, and secure enterprises from endpoint vulnerabilities, like information leakage and data theft, allowing for secure use of removable media and portable devices.

TABLE 2

Notable Israeli IT Security Companies

Company	Field	Description
ConTrust	Web security	Allows Websites and media platforms to control, detect, and filter User-Generated-Content (UGC) risks and threats, including spam, malware, and phishing content.
Covertix	IPC	Software technology that enables organizations to track, monitor, and control documents and files within and outside the organization.
Cyber-Ark	IPC	Digital vault solutions that provide secure infrastructure for sensitive cross-enterprise data exchange, secure storage and management of sensitive documents, and secure management of user passwords.
DynaSec	GRC	Web-based platform for managing GRC processes, allowing companies to build and maintain a framework in which each GRC project can be managed autonomously, while sharing relevant information with the other projects running in parallel.
Discretix	Mobile security	Embedded security solutions for mobile devices and flash memory, combining hardware, middleware, and software.
Finjan	Web security	Secure Web gateway solutions that protect against crimeware, malware, and data leakage, based on the company's active real-time content inspection technologies and optional anti-virus modules.
ForeScout	Network security	Provides clientless network access control (NAC) and policy compliance solutions, as well as protection against zero-day viruses and worms.
Fraud Analyzer Systems	Anti-fraud	Anti-fraud solutions that locate and prevent fraud, money laundering, and the transfer of funds to terror groups.
GamaSec	Web security	Online Web vulnerability scanner that tests Web servers, Web-interfaced systems, and Web-based applications against multiple vulnerabilities.
GED-I	IPC	Security solutions for storage devices, SAN, NAS, DAS, and tape, which utilize multi-layered security, encryption, proprietary structuring, and interference to recovery tools.
GRSee	GRC	Centralized platform for managing GRC processes.
Guardium	IPC	Database security solutions that provide visibility and control over database access activities. The company's products include database security assessment, access policy control and enforcement, auditing, and regulatory compliance.
HackStrike	Network security	Integrated network appliances that combine UTM and network-based DLP capabilities to protect against various insider and external threats.
HexaLock	Digital content protection	Digital copy protection solutions that are aimed at preventing unauthorized copying of digital content, when stored on optical or other digital media.
Imperva	IPC	The company's solutions provide data security, data assurance, and regulatory compliance for sensitive and proprietary data in corporate databases and web applications, covering both insider threats, external attacks, and malware threats.
Insightix	Network security	Agentless IT visibility and NAC solutions that provide comprehensive network coverage for network security, IT operations, and regulatory compliance.
Intellinx	IPC	Behavior-tracking solutions for protecting against insider threats, including internal fraud and information leakage, while complying with government regulations that include GLBA, HIPAA, Sarbanes-Oxley, and Basel 2.
mConfirm	Anti-fraud	Fraud prevention solutions for credit and debit cards. The company's products are aimed at combating point of sale (POS) and ATM fraud.

TABLE 2**Notable Israeli IT Security Companies**

Company	Field	Description
Meganet	IPC	The company utilizes symmetric encryption algorithm, which uses data mapping technology to create random cipher text to protect against hackers, internet theft, and internal sabotage.
NDS	Digital content protection	NDS is a provider of open end-to-end digital pay TV solutions for the secure delivery of content to television set-top boxes, PCs, and IP and mobile devices.
New Global Markets	Anti-fraud	Anti-money laundering and counter-terror financing solutions for the financial market.
n-Trance Security	Biometrics	Biometric security solutions for private and corporate users addressing various data security, identify theft, hacking, and other concerns.
ObserveIT	GRC	Software solutions that visually track and record user activities on enterprise servers and workstations – for regulatory compliance and security purposes.
PerSay	Voice authentication	The company provides various real-time authentication solutions based on voice biometric technology.
PineApp	Network security	eMail perimeter security appliance that protects organizations from viruses, spyware, and other threats, and allows enforcement of corporate surfing policies using content filtering tools.
Profitect	Anti-fraud	Loss prevention, fraud detection, and compliance reassurance software solutions that operate by analyzing data from various sources and detecting suspicious situations and patterns in real-time.
Promisec	GRC	Clientless endpoint security management solutions, also offered as managed services that detect and protect against internal threats while enabling effective enforcement of security policies.
Puresight	Web security	Internet content filtering solutions that analyze and categorize Internet content in real-time, to ensure its compliance with corporate, institutional, or parental acceptable use policies.
Radware	Network security	Integrated application delivery solutions that also address network security concerns. The company's security solutions include content security, DoS protection, intrusion detection and prevention, fraud detection, and VoIP security.
Raz-Lee	Network security	Software security solutions and tools for AS/400 (iSeries) networks, which create, monitor, and control the network firewall, green screen environment, passwords, and the audit trail.
Safend	IPC	Endpoint security solutions that allow organizations to gain visibility, control, and protection over their endpoints – exposing existing and potential threats, and enabling comprehensive data security.
SandBoxie	Web security	Sandboxie addresses zero-day virus and spyware vulnerabilities using a virtual sandbox that allows users to run programs in an isolated space, preventing them from making permanent changes to other programs and data in the computer.
Secure Islands	IPC	IPC solutions for securing sensitive enterprise information anywhere through central governance. The company's solutions are based on embedding encryption and policy into the information itself, while eliminating the need to secure the channels or the mediums.
Sentrigo	IPC	Database security solutions for protecting against intrusion, data theft, attacks, and other threats. The company's solutions operate by monitoring all activities on the database, including the activities of authorized and privileged users.
SentryCom	Voice authentication	Multi-factor, strong authentication solutions that verify a person's claimed identity based on voice recognition.
Simplima	Digital content protection	DRM solutions for protecting digital content from mass piracy, enabling lending and secure content usage by the intended recipients both online and offline.

TABLE 2

Notable Israeli IT Security Companies

Company	Field	Description
Skybox	GRC	GRC solutions that provide organizations with continuous view of risk while validating control effectiveness and compliance.
Snapshield	Mobile security	Encryption-based secure communication solutions that support quad-band GSM and standard smartphones, as well as analog and digital phone and fax equipment. The company also provides solutions to protecting mobile data, both at rest and in motion.
Trusteer	Web security	Web security solutions that protect online businesses from client-side identity threats such as phishing, pharming, and crimeware, which are targeted at consumer vulnerabilities.
Trustware	Web security	Application virtualization technology that transparently redirects modifications in a PC to a virtual, isolated environment, and thus enables secure download, importing, and sharing of programs and files.
Tufin Technologies	Network security	Network security lifecycle management solutions that are aimed at providing visibility and control for network security change and configuration processes.
Vanadium	GRC	GRC solutions that allow users to continuously detect and evaluate vulnerabilities, while enforcing compliance with both corporate policies and regulatory requirements such as SOX, PCI, HIPPA, and others.
Varonis	IPC	Unstructured data access control solutions that are aimed at ensuring that data is only accessible by the right users, reducing overly permissive access and associated risks.
Waterfall	Network security	Waterfall's unidirectional technology enables secure data transfer to or from corporate networks at the hardware level, addressing network security, DLP, data protection, and regulation compliance.
WhiteCell	Mobile security	Security and management solutions for wireless Internet and mobile data networks, which allows users to control and filter both current and future mobile data, as well as supporting technologies such as SMS, WAP, GPRS, and 3G.
White Cyber Knight	GRC	White Cyber Knight allows users to manage IT risk in real-time from a business-process perspective, providing a risk map driven by human behavior, policies and regulations, system architecture, technical vulnerabilities, and other factors.
WonderNet	Digital content protection	Biometric signature authentication solutions that incorporate digital handwritten signature capabilities into commonly used applications, to ease and secure document-signing processes.
Worklight	Web security	Customized and personalized Web 2.0-style secure access to corporate data residing in enterprise applications. The company also addresses security concerns that stem from the use of RSS, Ajax, widgets, and other Web 2.0 technologies.
Yoggie	Mobile security	Hardware/software security appliance that – by plugging it into a laptop, home computer, or home network – combines security applications with proprietary technologies to protect laptop users against various malware attacks.

Source: IDC, 2009

ESSENTIAL GUIDANCE

IT security is on the verge of a significant paradigm shift, from a network-focused and perimeter-centric stance to embracing environments that are data-focused and information-centric. In practice, this evolution is highly dependant on the emergence of new security concepts, technologies, and solutions. While global IT security continues to consolidate, mainly reflecting the increasing convergence of common security functionalities, innovation will still be in high demand for addressing the emerging challenges. Established players and start-up companies are both likely to drive much of the innovation required to realize this vision. Given its background and core capabilities, the Israeli IT security industry is likely to play a key role in this effort.

LEARN MORE

Related Research

- ☒ Central and Eastern Europe Security Software 2008–2012 Forecast and 2007 Vendor Shares (IDC #ESE1Q)
- ☒ Gulf States Security Software and Appliances 2008–2012 Forecast and 2007 Vendor Shares (IDC #ZSE1Q)

Synopsis

This IDC study analyzes emerging IT security trends that will reshape the industry in the coming years. Among other things, it discusses the need for organizations to focus on protecting the information itself rather than merely the perimeter, which is driving demand for new technologies in areas such as data loss prevention, secure collaboration, governance, and risk and compliance. At the same time, common security functionalities that are more network-focused and perimeter-centric are increasingly converged and outsourced to managed security service providers in order to reduce operational complexities and costs.

The study also discusses the opportunities for IT security start-up companies to capitalize on these emerging trends and specifically for Israeli companies in this space.

"Historically, Israel has served as a center of innovation for the global IT security industry, as in the cases of firewall and network security, encryption, and others. Looking at the current activities of Israeli security start-up companies can therefore help shed some light on the future of IT security." – Research Director Dan Yachin, IDC EMEA Emerging Technologies

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2009 IDC. Reproduction without written permission is completely forbidden.