GIGAOM RESEARCH

Cloud security market landscape, 2013–2017

Keren Elazari

a cloud report

GIGAOM RESEARCH

Cloud security market landscape, 2013–2017

06/10/2013

TABLE OF CONTENTS

Cyberthreats are now a critical issue affecting the national security of nation countries worldwide. This is thanks to a few factors: the rise of cloud computing and big data and the sometimes unclear virtual boundaries caused by increasingly mobile enterprises, among others.

In conjunction with the shifts mentioned in the previous section, the IT world is also witnessing a wave of new innovation, and there are numerous business opportunities for technologies built around the emerging market sectors of mobile and cloud computing. The cloud-security space itself is undergoing an intense maturation phase after a couple of years in a vague initial hype phase.

This report will examine:

- The difference between security *for* the cloud and security delivered *by* the cloud
- Market opportunities tied to the rise of IaaS
- Key technologies that address security needs for both public and private clouds
- Emerging business models and companies to watch

Introduction: the global cybersecurity industry's evolution

In the past few years, the cybersecurity industry worldwide has witnessed three major shifts.

The first and most influential is the rise of cyberwarfare and cyberespionage campaigns, nicknamed by industry experts as advanced persistent threats (APTs). Since 2010, or "the summer of Stuxnet," and the advent of Stuxnet, Duqu, Flame, and other campaigns, it has become clear that cyber threats are a critical issue affecting the national security of countries worldwide. Many governments have sought to form military cybercommands and national cybersecurity centers, including computer emergency readiness teams (known as CERTs, such as the U.S. government's CERT), security operation centers (SOCs), and military cybercommands. Lawmakers worldwide are pushing for advanced cybersecurity regulations, controls, and government investments.

The second shift is the demise of the perimeter, due to cloud and mobile computing along with big data. As more organizations worldwide seek to leverage the efficiency and agility of these technologies, the classic enterprise, with on-premise IT infrastructure and server farms, has quickly transformed into an extended enterprise with virtual — and sometimes unclear — boundaries between corporate-owned and corporate-managed computing resources. IT is now consumed as a service (SaaS, IaaS, or PaaS), and data resides on a multitude of different devices, some belonging to the employee and some to the corporation. This bring-your-own-device (BYOD) trend coupled with the fact that mobile workers travel all over the globe mean that connected technologies are extending the boundaries of where corporate data is processed, stored, and transmitted.

Cloud services, web applications, and the extensive use of social media platforms by organizations also create a new reality where the enterprise boundary, once easily defined by an IP address range or even an autonomous system (AS), is now completely broken: technologies (firewalls, gateways, intrusion detection systems) that were once prerequisites for any IT environment. These are still required but slowly losing relevance, because they are no longer effective in stopping data breaches or even employee misuse of corporate information and infrastructure. And with huge amounts of data generated by corporations but stored and processed elsewhere, the fight seems to be already half lost.
Finally, the bad guys are gaining the upper hand. Cybercrime and corporate espionage attackers are persistent, and they only need to get past protected organizations' perimeters once — while defenders are racing to plug a seemingly endless amount of security holes. This trend is alarmingly clear: Three years ago, zero-day vulnerabilities were considered rare, and they were traded on the black market for thousands of dollars. Only top-notch cybercrime syndicates and state-sponsored espionage campaigns were using such expensive cyberweapons. This is no longer the case. Unpatched software vulnerabilities are discovered weekly in prominent software platforms such as Java and Flash, leading to widespread panic in the software industry, as these bugs are used to infiltrate companies like Facebook, Apple, and Twitter in recent months.

Meanwhile sophisticated malware is outsmarting defensive mechanisms with self-mutating, polymorphic codes and evasion techniques that are designed to bypass most security systems. Recent findings by

security vendors and malware research labs show "unprecedented levels of polymorphism" within examined malware samples. This means that while cybercriminals are evolving, detection rates by commodity antivirus software and other end-point protection mechanisms are falling fast.

Market overview: trends, innovation, and new business models

In conjunction with the shifts mentioned in the previous section, the IT world is also witnessing a wave of new innovation, and there are numerous business opportunities for technologies built around the emerging market sectors of mobile and cloud computing.

The cloud-security space itself is undergoing an intense maturation phase after a couple of years in a vague initial hype phase. Startup companies including Skyhigh Networks, Seculert, and Incapsula, as well as leading cloud-security services offered by cloud-security pioneers such as CloudPassage, CloudFlare, and Zscaler, are creating interesting business models built for the cloud with security technologies and approaches that are worth a closer look. And with data breaches on the rise and corporate IT moving to the cloud slowly but steadily, it is important to understand the security implications around these technology shifts now rather than later. This report examines what's new and emerging in this space, and it explains the difference between security for the cloud and security delivered by the cloud. It also highlights emergent leaders in this dynamic, multibillion-dollar industry technology category.

Cloud security: from adoption concerns to business enabler

Many forward-thinking organizations and businesses today recognize the cost benefits and agility of using cloud-computing resources, but many are still hesitant to make the transition to the cloud. Specifically, companies operating in sensitive market sectors such as health care, finance, defense, and others primarily state concerns over security, consumer data privacy regulations, and compliance with other industry standards and regulatory requirements as their reasons against cloud adoption. Hence, security concerns have become the No. 1 inhibitor of wider-spread cloud adoption, as witnessed by recent industry surveys and reports that list security as the top concern slowing down cloud deployments.

However, with popular web applications, collaboration platforms, storage solutions, and the bring-your-own-device movement across organizations, corporate data is already stored outside classic IT environments. So many companies are in fact already operating in the cloud and are simply unaware of that fact. That's where cloud-security technology vendors come into the picture: By addressing the gap between traditional IT departments' understanding of the cloud and what's really happening in the organization, such companies have managed to create a new role for cloud-security solutions. This will eventually legitimize employees' use of cloud resources and bring them under the extended enterprises' security umbrella.

Market opportunities: the rise of IaaS

The market is currently experiencing the rise of Infrastructure as a Service (IaaS), thanks to continued growth in cloud adoption and an expected double-digit rise in global spending on cloud services. In IBM's 2012 global "Tech Trends" report, more than 75 percent of over 4,000 IT professionals surveyed confirmed the following finding: More and more organizations will leverage cloud-based infrastructure (IaaS) to do more business more efficiently and save on the bottom line of major IT expenditure. With that, we expect to see more data centers and cloud-based server farms, which require their own set of security technology solutions and services.

On the infrastructure front, we expect to see more of the following offerings come into play in the market.

Managed security service providers (MSSPs)

MSSPs will offer more security services from the cloud, building full suites of advanced security services delivered completely by the cloud. These services include security-configuration management, advanced malware detection, log analysis, incident response, forensic analysis, and more. A notable example is SilverSky(formerly called Perimeter Interworking), a rebranded MSSP venture that combines established managed service provider Perimeter E-Security and USA.net into one mammoth provider that offers a broad range of managed security solutions and cloud-security solutions. SilverSky pioneered concepts of

remotely managing security as early as 2000, with Perimeter's founder actually patenting its "security in the cloud solution."

Telco-grade security appliances

These will enable communication service providers (CSPs) — including traditional telco and also wireless, mobile, and leased-line infrastructure providers — to broaden the meaning of ISP and offer cleaner pipes at a premium cost. Doing so will provide a relatively more secure alternative to commodity ISPs.

Security for IaaS

Security controls for the IaaS market will provide on-demand additional security on top of the basic offerings available today. These will follow scalable pricing models to address the changing market needs of elastic cloud IaaS customers. With massive public cloud adoption, typical IaaS consumers control only a sliver of the infrastructure they actually use. The underlying computing, network, and storage infrastructure remain under provider control. Nonetheless, IaaS consumers still shoulder the responsibility for implementing and upholding security requirements such as strong authentication, OS level hardening and controls, log analysis and auditing capabilities, and file-system encryption.

Government-managed and -regulated secure ISP for selected market sectors

The American government's Trusted Internet Connections (TIC) initiative was created, according to the Department of Homeland Security (DHS) website, "to optimize and standardize the security of individual external network connections currently in use by federal agencies." The TIC model mandates that federal agencies use approved ISPs and regulates security requirements. Previously federal agencies chose independently from hundreds of localized service providers. They now use centrally selected and certified trusted ISPs called managed trusted internet protocol services (MTIPS). The federal government's central department for cybersecurity issues within federal agencies has also created a list of TIC-compliant solutions providers that federal agencies can contract in order to be fully compliant with the new security requirements put forward by the office.

Another example is the Australia-based icode project, which is perhaps the first example of a successful public-private partnership effort. The project marks the advent of voluntary participation for ISPs in government-coordinated projects. In 2010 the Australian government partnered with the Internet Industry Association of Australia to create a system for ISPs to actively detect consumers' computers that are infected with malware, then redirect those affected users to a closed-garden environment where information and tools about removing malware is made available. The icode project has been set up specifically in order to "promote a security culture amongst the internet industry by reducing the number of compromised computers in Australia," and officials have said it is helpful in reducing the spread of malware within Australian internet subscribers, with "most customers grateful for being told of infection ," according to Bruce Matthews, the manager of e-security operations with the Australian

Communications and Media Authority. The project is also helping ISPs to cut costs associated with handling massive botnet infections that adversely affect bandwidth consumption or use infected computing resources for spam circulation, which can lead to IP address ranges becoming blacklisted on the web.

Market opportunities: return of the TLB

As chief security officers in organizations learn how to take back control of the cloud, we expect to see IT security staples and basic building blocks get extended into the cloud, bringing back the three-letter buzzword lists of enterprise security that have dominated the industry over the past decade. These are technologies that address fundamental security needs for most large enterprises, and more of these will be coming to private and public clouds:

- Single sign on (SSO), identity and access management (IAM and IDM), and multifactor authentication (MFA)
- Data leakage prevention (DLP)
- Intrusion detection and prevention systems (IDS and IPS)
- Web application firewall (WAF), protecting websites from web attacks on the application layer such as SQL injection, cross-site scripting, and more
- Log management and analysis, security incident and event management (SIEM)
- Encryption for data at rest, in transit, and stored with third-party cloud providers
- Database management and security solutions
- Server-side security and hardening for IaaS-deployed servers

Emerging cloud-security business models and companies to watch

The following sections include a discussion on new business models in the cloud service space and also those companies creating these new models and technologies.

Cloud-delivered security vs. security for the cloud

Some IT security technologies and services were delivered over the web in the past, with companies offering email proxies for anti-spam filtering and web traffic inspection for distributed denial of service (DDoS) protection for more than 10 years. Notable examples include Prolexic, which has been providing DDoS protection for websites, and Postini, which has been owned by Google since 2007 and since 2013 has been part of the Google Apps portfolio. These cloud-based anti-spam solutions for corporate email systems have existed since 2005.

One could even say that such solutions have been delivered by the cloud for more than a decade. But now the time is ripe for advanced security solutions that might replace classic IT security departments within organizations and actually provide value to smaller organizations that once could not afford such a notable investment in security. In fact, with the current communication speeds and cloud-based computing resources, it is now more cost-effective to apply security controls on a much larger scale, leveraging the accumulated expertise of security vendors that are capable of processing hundreds of gigabytes of traffic and web transactions every second. With that, we expect to see more edge security services deployed on elastic and scalable clouds, at the CSP, data center, and cloud provider levels.

At the same time, industry innovators, startups, and even IT security market leaders are offering more cloud-powered security solutions and bringing the cloud into the enterprise. In the following sections, we discuss some of the emerging business models and different technology solutions under the cloud-security umbrella.

The classic Security as a Service

CloudPassage is one of the pioneering companies at the moment, and it offers a wide range of classic security in a SaaS model. The company's offering includes vulnerability assessment, security monitoring, two-factor authentication solutions for cloud-based data assets, and event logging and alerting. Its initial market traction was established when the company began offering a freemium model as well as providing a much-needed solution for two key market segments: SMBs and startups operating in the cloud and distinct departments within large companies that wanted to use cloud services without going through corporate IT. The common feature between these groups: Both wanted to start using the cloud securely, efficiently, and quickly. They wanted to do so without worrying about data breaches, losing intellectual property in the process, or, most convincingly, without going through traditional IT cycles of lengthy and expensive purchasing and deployment processes. CloudPassage offers security for the cloud, by the cloud, and it is gaining broad recognition as a market leader within the Security-as-a-Service category.

Skyhigh Networks came out of stealth mode in early 2013 with a clever approach: It provides visibility about cloud services already being used by organizations. Its unique value is its risk-measuring and dashboard system, which creates detailed views for CIOs to regain control of corporate IT that has

migrated to the cloud. Skyhigh also feeds into the existing security ecosystem by creating configuration settings for most perimeter security solutions. In this way much of a CIO's job is automated. Skyhigh's approach of helping CIOs discover shadow IT is actually already being used by corporate employees, and the service measures the risk levels of those services by offering basic tools to mitigate them. This represents a valuable time- and cost-saving combination for CIOs.

Zscaler Security Cloud is a cloud-delivered, Security-as-a-Service offering, or what is essentially a web-security gateway for SaaS traffic. Zscaler has been one of the pioneers of the "security by web proxy everything" approach, which allows it to provide application controls, traffic inspection, and policy enforcement for outbound web traffic and shaping capabilities. Zscaler combines the major traffic-management capabilities with much-needed security features, such as malware detection and integration with other building blocks of security delivered from the cloud, such as IDM as a Service from Okta.

Okta is a young yet rapidly growing startup. It was founded by industry veterans and has developed an impressive customer base for its cloud-based offering of IDM, SSO, and provisions for SaaS applications. Okta could be described as delivered for the cloud and by the cloud, as it uses AWS, running a single-instance multitenant service. Okta is widely used by many SaaS providers as their full directory service and identity management system. The company offers a simpler way for organizations to implement IDM, SSO, and provisioning through the extended enterprise (cloud, mobile, anywhere). It also helps organizations roll out more web services and integrate with additional SaaS easily. Companies like Okta might be the redemption for IDM and SSO because they provide a simple solution that is much needed by enterprises. This replaces the dreaded, complicated, and often failed on-premise implementations of classic enterprise IDM solutions.

Cloud-delivered website security solutions

These cloud-based security solutions require routing website traffic through the provider's data center or a global network of servers for filtering and analysis. While computing resources and bandwidth have become commodities, there are clear economic rationales and benefits for delivering web Security as a Service in a cost-effective way. The following players have been disrupting the security industry's classic business models.

Incapsula

Perhaps the pioneer in providing low-cost, highly needed website protection for SMBs via the cloud, Incapsula leverages the biggest brand in enterprise-grade web application firewalls but is more of a classic security vendor and less of a CDN. Incapsula is actually a spin-off company of global web application firewall (WAF) leader Imperva. It aims to provide even the smallest of websites with cost-effective, enterprise-grade web security as well as DDoS protection and bandwidth-optimization benefits. Incapsula competes directly with CloudFlare (discussed below), which offers similar security features with a bigger content-delivery network at a lower price point. The fact that Incapsula leverages the vast

web application security expertise and brand recognition accumulated over the years by Imperva helps position it at the top of the game, despite a higher price point.

CloudFlare: from protecting hactivist websites to Fortune 500 clients
CloudFlare was one of the first companies to call itself a security cloud service provider.

CloudFlare offers Security as a Service for websites. Its website DOS protection and web application firewall offering is growing in popularity, and CloudFlare now says that a substantial percentage of the world's global web traffic travels through its infrastructure daily. According to CloudFlare, in 2011, " 12% of the people on the Internet have passed through CloudFlare's servers" and in 2012, its infrastructure saw more web traffic than "Amazon, Wikipedia, Twitter, Instagram, and Apple combined." Surprisingly, CloudFlare's first business came from many small, previously unprotected websites. It was initially developed as a tool to increase website security but was later discovered to also enhance website loading times rapidly. The company now serves ecommerce websites, top media websites like the European Broadcast Union's Eurovision website (which has more than 150 million viewers), U.S. financial organizations, and even WikiLeaks. CloudFlare's top differentiators from Incapsula are its global CDN, the sheer size and speed of its data center network, and the collaborative usage of collective security intelligence gathered about web attacks targeting its entire user base.
Some independent security researchers have evaluated and compared CloudFlare and Incapsula's offerings (PDF) and found them far from being on par. Incapsula gains an edge on the technology side, but content delivery and optimization is where CloudFlare wins.

Both companies compete with Akamai, the industry's leading CDN, which offers its own brand of Kona Site Defender, a cloud-based website protection and DOS prevention solution with web application firewall (WAF) capabilities and network layer controls. Akamai also built in features and APIs to allow its solution easy integration with on-premises security solutions or to be controlled remotely by managed security services providers (MSSPs), which configure and monitor websites for multiple customers.

Security solutions powered by the cloud

CrowdStrike

Founded in early 2012 by senior security industry luminaries, CrowdStrike is now building its active defense platform, branded CrowdStrike Falcon. The company's goal is to detect advanced cyberthreats that traditional security technologies can't find — namely, the "advanced persistent threat" type of cyberattacks such as the infamous Operation Aurora data breaches into U.S. software giants Google and Adobe in 2009 or the Night Dragon APT, a global campaign designed to steal sensitive data from targeted organizations in the energy and gas exploration sector. These types of highly sophisticated, specialized, and targeted attacks have become a common problem of the security industry in recent years, bypassing existing security layers by using unknown attack tools and techniques that common defensive technologies fail to detect. CrowdStrike's approach of proactive security after detection is part of a larger paradigm shift

in both the public and private sector toward deploying active defenses against cyberattacks, compelling breached organizations to do more about these types of attacks.

Upon detecting the breach or the infection, CrowdStrike seeks to provide the affected organizations with a range of active response measures that are designed to raise the cost of successful entry for attackers. The product misleads attackers in various ways. Examples include sending fake information that lures attackers to honeypot environments or tracking information about the command and control servers that attackers use. At that point, CrowdStrike moves for legal action with ISPs to take those servers down. CrowdStrike's approach is innovative, as it fuses findings from data analytics with high-resolution intelligence about cyberthreats and adversaries. That intelligence is then painstakingly collected. The analytics happen in the CrowdStrike cloud, which correlates intelligence and security events in real time from its global network of sensors. Intelligence about analyzed attacks is then disseminated throughout the collective community of its customers' base.

Seculert

Israel-based startup Seculert's cloud-based analysis engine has already won the company accolades for succeeding where others fail to detect cyberattacks. It discovered the now infamous Mahdi, Shamoon, Dexter, and Red October malware, sometimes beating established security companies to the punch. Seculert uses cloud platforms to analyze vast amounts of data, comparing malware samples and traffic collected from its customer base as well as additional sources. Findings are accessed via a web interface and are integrated with on-premises intrusion detection systems to automate threat prevention. Seculert's offering is focused on helping organizations that have already been breached but don't realize it. Today's corporate IT environments continually face the growing chance of being widely infected by botnets and other malware. Seculert's service is perhaps the easiest way for IT managers and chief information security officers (CISOs) to actually find out where all of their existing security technologies have failed them and then move swiftly to clean up those infected machines. The bottom line is that Seculert helps companies discover these failures, which might have otherwise gone unnoticed for months — or even years — as recent data-breach-investigation reports have demonstrated.

Security for web applications and Software as a Service

Many of the vendors operating in this space offer data- and communication-encryption solutions for enterprises using popular SaaS and web applications. Several vendors have already established themselves in specific SaaS ecosystems and popular cloud infrastructure (IaaS) and cloud platforms (PaaS).

These are the most important differentiators in this category:

- Ability to keep data searchable and usable within web applications (e.g., by maintaining important application-specific fields within the data)

- End-user transparency and ease of deployment
- Encryption keys management and key separation
- Additional security controls and capabilities offered on top of encryption
- Compliance with industry-specific data-protection regulations and standards

CipherCloud

CipherCloudsecures popular cloud applications, including Salesforce.com, Force.com, Chatter, Gmail, Office 365, and Amazon Web Services. Its main focus is offering encryption for data that is transmitted out of the organizations. CipherCloud does so by plugging into the client's existing on-premises security gateway. This simplistic approach of deploying encryption on the fly is helpful in maintaining data usability, as data is converted to plain text prior to being displayed to the end user. CipherCloud's popularity (it currently claims to protect more than 100 million customer records) demonstrates that not everything that corporate uploads to the cloud has to be encrypted. Rather, corporate IT departments can choose to implement protection policies for selected information streams or data types. This hybrid protection approach enables cost-effective compliance with data-protection regulation like HIPAA. However, CipherCloud should not be viewed as delivering a full-blown cloud-security solution. It offers a split cryptographic key management scheme, by which encryption keys are stored with CipherCloud but are managed by customers — a solution that some organizations might find trickier to manage and maintain.

Porticor

Porticor was one of the first vendors to offer encryption for cloud computing resources. ItsVirtual Private Data offering focused on volume-level encryption for cloud-based storage. Porticor's approach to the questions of key management was to implement split-key encryption technology, which ultimately leaves full control and responsibility for encryption keys with the customer, not the cloud provider. Porticor was one of the first to offer scalable encryption at a low price point for cloud storage. Its offering isn't niche or custom-designed but rather should be understood as a basic commodity, priced as such, making basic protection of corporate IP reasonable for even the leanest of startups.

Vaultive

Vaultive is a somewhat new player, coming out of stealth mode late in 2012 to offer cloud-encryption solutions. It focuses on encrypting data in ways that do not break the applications that use it, meaning information is searchable even as it is being encrypted and stored in the cloud. Similar to its competitors, Vaultive keeps encryption keys that are separate from the data but remain inside the Vaultive product. The company offers an enterprise-grade product designed to support the most popular web applications used by businesses such as Microsoft Exchange, Office 365, and offerings from Salesforce.com. Its goal is to provide an elusive yet much coveted combo of safe, compliant, cloud-based business products that are easy to use and also feature transparent security to the end users. Vaultive also has a strong R&D team based on Israeli security talent and CEO Elad Yoran at the helm. That's a winning combo, and the fact that Vaultive has managed to secure a Microsoft endorsement and partnership relatively early in the

game for such a young company attests to the faith bestowed upon it by the SaaS industry.

Navajo Systems (acquired by Salesforce.com in 2011)
Israeli cloud-security startup Navajo created a virtual private SaaS (VPS) technology that was designed to run corporate networks and as a proxy server among browser agents (and other components that interact with the SaaS application) and the SaaS application server. The purpose is to encrypt data before it is transmitted outside corporate networks. In 2011 Salesforce.com acquired Navajo for approximately $30 million. This marked possibly the beginning of a larger consolidation and M&A trend, whereby large cloud and SaaS providers seek to acquire innovative startups that can easily integrate security capabilities on top of their offering, bolstering their security appeal with existing and potential customers that still harbor security concerns. And with software giants like SAP and Oracle bounding into the cloud market with the 2012 acquisitions of Ariba, SuccessFactors by SAP, and Taleo and RightNow by Oracle, there is a lot of money at stake, hinging on the trustworthyness of these business-oriented cloud platforms. Some of the following smaller companies, focused on solutions for specific cloud ecosystems, might find themselves as such potential M&A targets:

- **CloudLock.** Security for popular Google Apps
- **PerspecSys.** Security for Salesforce.com
- **Dome9.** Firewall management for servers deployed on Amazon's EC2

Network security appliances evolve and leverage the cloud

Several leading network security players have already brought the cloud into the enterprise by coupling powerful network-processor-based appliances that offer threat detection at line speeds with cloud-based threat intelligence feeds and malware-analysis capabilities. This essentially fuses the classic firewall with cloud-powered threat intelligence.
Check Point's ThreatCloud infrastructure offers managed security services for Check Point appliances and threat mitigation: a combo of cloud-powered security services with the industry's gold standard of firewalls.

Check Point's fiercest competitor, Palo Alto Networks, now offers a cloud-based WildFire solution, which is a malware-analysis platform based on sandbox testing. Essentially it transposes FireEye's popular malware-identification approach to the cloud, thus effectively combining Palo Alto Network's next-generation firewall with the latest trend in cloud-based malware analysis. At the same time, FireEye itself also offers Malware Protection Cloud, an online service that collects and shares threat intelligence about emerging malware and cyberthreats among FireEye malware-detection appliances deployed worldwide.

And the real testament of firewalls taking to the cloud is FortiCloud, a hosted security management and

log-retention service offered by Fortinet that is designed to service its FortiGate line of firewall appliances. It's the first cloud for firewalls, which is almost a counterintuitive concept.

IT giants extending existing technology offerings to the cloud

The aforementioned network security players have stayed on edge with the dynamic developments in network speeds, bandwidth consumption, protocols, and more, making the move to include cloud technologies in the basic firewall offering. This is a natural, organic transition for most. Still, the traditional enterprise IT and end-point protection giants are having a harder time adapting to the cloud and its impact on their business lines. Naturally, the biggest players in the security industry, which made their fortunes protecting millions of end-point devices, are trying to create new versions of existing products to extend their market reach into the cloud while protecting their enterprise customer base. Notable examples include:

- McAfee Cloud Identity Manager, which enforces corporate security standards for cloud applications
- Symantec Cloud Services, which offers cloud-based email encryption, email security, web security, and IM protection
- Trend Micro SecureCloud, which offers data encryption and a security umbrella for public and private clouds and virtual environments
- CA's CloudMinder, which extends existing corporate identity management to the cloud

Some of these efforts might be good enough to be seen as genuine products designed for the cloud, but a lot of them are actually repurposed and retooled existing technology by tech giants that have lost their edge. These multibillion-dollar players are shuffling now in a hurried attempt to bring their complicated, enterprise IT, glacier-like products to the cloud. Many of the cloud-security solutions from these players might turn out to be revamped versions of existing technology that have been slightly modified but not built for the cloud. We expect these vendors to eventually attempt to acquire and integrate some of the up-and-coming startups in this field. Therefore, companies that truly focus on securing the extended enterprises within the cloud context that have a core technology offering that is complementary or synergistic to these giants will become attractive M&A targets or technology partners. Overall, we expect cloud security to represent a major theme for M&As by these IT and data-storage giants.

Bringing cloud and mobile security together

With the advent of the BYOD movement and mobile computing, it is of note to discover the new approaches of solution vendors that have chosen to harness the power of the cloud to deliver security for mobile applications.

Because web-based mobile applications are so prevalent, it has become viable to use cloud platforms to create risk-scoring metrics and security testing for popular mobile applications. This represents a valuable and scalable solution for security-conscious organizations that still need to enable employee use of third-party mobile applications. A notable example of such a solution provider is Appthority, which is a mobile application reputation startup that uses a cloud-based platform to deliver what it refers to as "mobile application risk management." Its solution competes directly with Veracode, an application risk management provider that also acquired Marvin Mobile Security in order to bolster its stable of cloud-based mobile application security testing. Atlanta-based startup Ionic Security, meanwhile, represents the next generation of cloud-security vendors. It recently raised $10 million, listing Google Ventures as one of its backers. Its vision is to unify cloud security with mobile security to create one holistic solution that will combine encryption and access control to protect sensitive data wherever it might be: in the cloud, on corporate devices, or on mobile devices, and data in all states, be that in transit, at rest, or at the end point.

Many companies talk of creating holistically managed security solutions that can address all the issues enterprises face in today's dynamic IT world. However, it remains to be seen who will be able to truly deliver value in the form of comprehensive solutions that are scalable, effective, and device-agnostic as well environment-agnostic. These offerings must also protect the extended enterprise everywhere, regardless of the previous corporate IT boundaries.

Final words: the future of security technologies

Will future security technologies all reside on the cloud, or is there still room for the traditional defense-in-depth layered security approach? Will the market still produce and require security delivered by software clients deployed at the end points, managed by on-premises servers and protected by network perimeter security appliances and network access controls? It seems that today's current reality is that not all corporate traffic is easily web-routable. Simply put, that means it might not be possible to shift entire information streams created by organizations today to the web and to filter all of that traffic through cloud-security providers without breaking the applications.

The current prevailing approach in today's IT world is to create hybrid solutions composed of on-premise IT with cloud-based computing resources. The same is true of security. The recommended approach is to create a balanced combination of effective protection mechanisms deployed on premises with the right powerful security technologies delivered by the cloud, at IaaS data centers, and ISPs.
We expect this trend to continue, with a focus on extensible security solutions that can be applied both for cloud services and traditional IT infrastructures and also address the expected growth of mobile device usage.

The defense-in-depth security paradigm will have to evolve to include cloud-security components. The existing need for end-point security solutions and next-gen security solutions will only continue to grow, creating demand for sophisticated solutions that can deliver security for the extended enterprise.

About Keren Elazari

Keren Elazari is a security expert, public speaker, and industry analyst with GigaOM, covering emerging technologies in mobile device security, cyberthreat detection, and cloud security. For more than 12 years, Elazari has been employed with leading security vendors, government organizations, and Big 4 and Fortune 500 companies in Israel.

Elazari has organized, hosted, and participated in international security events such as Y2Hack04 and ILHack09 in Tel Aviv, ITBN 2007 Security Day in Budapest, IDC Herzliya Cyber Terrorism Workshop in 2010, the NATO International conference on Cyber Conflict 2011–2013, and the RSA Conference in 2013. She has also been an invited speaker at international media events such as DLD, Campus Party, and Wired. During 2012 Elazari held the position of teaching fellow — Security with Singularity University, in Mountain View, Calif. She received a BA in History and Philosophy of Science and Technologies from Tel Aviv University and the international accreditation for Information Security professionals, CISSP, in 2007. Elazari is also a research fellow with Tel Aviv University's Yuval Ne'eman Workshop for Science, Technology and Security.

GIGAOM RESEARCH

About GigaOM Research

GigaOM Research gives you insider access to expert industry insights on emerging markets. Focused on delivering highly relevant and timely research to the people who need it most, our analysis, reports, and original research come from the most respected voices in the industry. Whether you're beginning to learn about a new market or are an industry insider, GigaOM Research addresses the need for relevant, illuminating insights into the industry's most dynamic markets.

Visit us at: pro.gigaom.com.