IDC Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

EXCERPT

Worldwide and U.S. Security Services Threat Intelligence 2011-2014 Forecast: Out of the Basement and into the Clouds

Christian A. Christiansen Charles J. Kolodgy
Chris Liebert

IN THIS EXCERPT

The content for this excerpt was taken directly from the Worldwide and U.S. Security Services Threat Intelligence 2011-2014 Forecast: Out of the Basement and into the Clouds by Christian A. Christiansen, Charles Kolodgy, and Chris Liebert (Doc # 230490). All or parts of the following sections are included in this excerpt: IDC Opinion, Situation Overview, Future Outlook, and Essential Guidance. Also included is Figure 1 and Table 1A.

IDC OPINION

The security services threat intelligence market is made up of advanced security event monitoring and management technologies that incorporate a variety of threat-related information sources to develop predictive security. IDC forecasts the size of this market in 2009 to be almost $200 million, with an expected CAGR of 35.5% from 2009 to 2014 to reach $905 million by 2014. Defined as a competitive market by IDC, security services threat intelligence is made up of vendors that provide products, services, or professional services (or a combination of these) to meet enterprise demands for advanced persistent threat (APT) solutions and actionable advice. While there are threat intelligence security products on the market, which we briefly describe throughout this document, that is not our focus. The main focus of this document is around security services vendor offerings for advanced global correlation and aggregation of events to preemptively detect security threats for their clients through a managed customer premises–based (CPE) or cloud service delivery platform. Threat intelligence services grew out of security services providers developing threat detection capabilities to address the challenge of detecting advanced persistent threats and other threats that are unknown, targeted, low and slow, and adaptive. Following are some of the threat challenges enterprises face today, which the security services vendors are attempting to address with their solutions:

- The speed with which threats are increasing (millions of malware variations for enterprises to defend against) make it increasingly difficult for signature-based antimalware to keep up.

- As signature databases grow to handle the variants, these large databases can impact client and server performance. Moreover, signatures only work for known vulnerabilities; they are largely useless against APTs because APTs are unknown and previously unseen.

Filing Information: November 2011, IDC #230490
: Excerpt

- The tendency of attacks to be short (lasting less than a couple of hours or only a few minutes) and highly targeted (e.g., specific URL, person, company, or IT asset) complicates detection, mitigation, and remediation.

SITUATION OVERVIEW

Current Security Threat Situation

Emerging Web application and other difficult-to-detect attacks are changing the security protection landscape and, subsequently, enterprise security posture. To ensure that enterprise network, application, data, and endpoints can remain secure (clean of malware and breaches), antimalware products and services are evolving to deal with these threats and reducing reliance on general signatures by instead adopting other forms of detection that we describe in this document.

IDC believes that the North American year-over-year growth rate for security services threat intelligence products and services grew 65% from 2010 to 2011 as enterprises looked to proactively monitor and mitigate malicious network traffic. This market is a combination of technologies called by a variety of names by the participating vendors, including predictive security, real-time threat management, situational risk awareness, or advanced SEIM.

Threat intelligence products and services incorporate proprietary heuristics and correlation techniques that analyze millions of global events to uncover malicious activities. Other technologies include IP and Web site reputation services that identify threatening and malicious content available on the Internet and blocking access to that content before it ever gets downloaded.

EMC/RSA aptly summarizes the threat situation in its latest Security for Business Innovation Council (SBIC) report released on August 2, 2011, as, "In the past 18 months, a string of highly sophisticated and targeted cyberattacks across the globe has revealed a seismic shift in the threat landscape." The report further states, "Traditionally only affecting the defense establishment, advanced persistent threats, or APTs, are now targeting enterprises in a wide range of industries."

Vendors providing advanced threat detection products or services across the security services threat intelligence market's ecosystem would say the same thing, and their data reveal the same findings as we discovered in our research with these vendors. Further, in addition to EMC's SBIC report, individual vendor summaries in the Competitive Overview section provide links to cybercrime reports released regularly by those security services vendors to describe the emerging threats and their solution for managing those threats. APTs create particular concern in the enterprise community as they are run by rogue actors, sometimes part of nation-state sponsored cybercrime. These malicious actors actively collaborate (and compete) with one another. The threat ecosystem has formal and informal structures and processes to sell, trade, and share zero-day vulnerabilities, weak assets, tools, detailed assessments, and techniques formerly available to government agencies.

Worldwide, malware writers are putting more effort into threat research, detection evasion, and mitigation of security defenses. With these new techniques, interchangeably shared within this community, attacks can be launched against a targeted "high value" enterprise with multiple attack vectors such as spam, spoofed email, social media, phishing, social engineering, and existing malware.

In the latter case, attackers can leverage existing malware and botnets to seize control of the system. In fact, the new attackers will often selectively patch the malware to enable their access but deny the original attacker. IDC strongly believes that there are no "minor" infections because all installed malware are vectors for more sophisticated attacks.

APTs are not the only real-time threat detection problem for the average enterprise today as signature-based tools (antivirus, firewalls, and intrusion prevention) are only effective against 30–50% of current security threats. Following are some further points to consider in the fight for real-time threat detection:

- Low-slow, polymorphic threats, applications attacks (e.g., PDFs and other file types), and Web-based threats (through Flash applications) fall outside the domain of traditional signature-based tools and are increasingly a problem for all businesses. As noted in Symantec's 2011 Threat Report, attackers are targeting SMBs as well as very large enterprises and government. Security is an increasingly larger portion of IT budgets, yet enterprises are in worse shape now, as noted by FireEye in its recent threat report. Companies expect the effectiveness of signature-based security to continue to decline rapidly, according to the latest IDC *Cloud Security Survey*.

- Ten years ago, government, financial services, and very large enterprises were the target of cybercriminal activity, but over the past five years, attacks have enlarged their scope to even commercial SMBs offering high-value targets (e.g., financial information, intellectual property, and other proprietary data). It is not just credit cards and source code anymore, information is the new worldwide currency. Every piece of data is valuable to someone, somewhere, somehow. Attackers are using data mining techniques (i.e., Big Data), virtualized servers, and cloud computing to improve attacks, analyze defenses, extract valuable trends, and break defenses (weak encryption, bad PKI, etc.).

- Many organizations, despite having implemented some of the more standard countermeasures (i.e., firewalls, antivirus, IDs) still do not have visibility across their environment to understand what is happening at any given time. While SIEM technology has significantly matured over the past five to seven years, a larger number of organizations today have nothing implemented or have solutions that are partially implemented without a proper security monitoring strategy in place. This makes it nearly impossible to really understand what is happening in their environment from a threat visibility and awareness perspective.

- Enterprises' awareness and sensitivity to these threats are high due to media coverage of high-profile attacks and subsequent high-value data losses to those organizations. However, many companies are more concerned with public relations issues from data breaches, not with the mitigation of risk. This short-sighted and erroneous perception that compliance equals security delights attackers.

- Resource constraints are always a problem. Only a few highly sensitive global enterprises and select government agencies can afford to fund their own threat intelligence operations. Worldwide, only the top banks and defense contractors like Northrop Grumman, Lockheed Martin, and Raytheon have this kind of IT and security staff.

- Financial services already seeing escalating zero-day attacks, hacktivism, industrial espionage, and insider attacks from within their global organizations will be a growing concern.

Security Services Threat Intelligence Definition

The security services threat intelligence market mainly started out in the form of threat advisories from ISS, CERT, SANS, and other antivirus and vulnerability assessment–oriented companies, then morphed into information/threat tracking sources such as incidents.org (crowd source–based top port/IP initiative), and has advanced into what we have today in Zeus and SpyEye tracker.

The security services threat intelligence as described in this document is made up of the following:

- Delivered through cloud-based portals and data libraries
- Based on behavioral detection and customer-specific signatures
- Sold as a data service, SaaS, and/or professional service
- Moving toward data feeds and solutions with analysis and mitigation

What security services threat intelligence isn't?

- Lists and generic signatures (that are not based on a particular customer's environment)

Market Drivers for Threat Intelligence as a Service

The threat intelligence–as-a-service market will be driven by enterprises' security defense challenges in the following areas:

- Detect and possibly counter APTs and other unknown threats.

- Reduce zero-day malware by providing early detection and near-real-time alerts for all monitored systems.

- Defend against professional criminal enterprises, industrial espionage firms, and government agencies engaged in disruptive activities (e.g., denial of service), fraud, espionage, and hacktivism.

- Relieve the stress of enterprises' and government agencies' inability to afford expansion of in-house threat intelligence research.

- Address the increasing need for more data from external sources with worldwide data correlation and possibly some analysis and mitigation recommendations. Rich contextual analysis of threat events from external sources of global intelligence and analysis along with mitigation recommendations is required by enterprises today.

- Counter ineffective behavioral analysis at the perimeter to avoid targeted and distributed denial of service (DDoS) attacks.

- Add some elements of data loss prevention (DLP) via detection of compromised systems and exfiltrated data and documents, but in passive mode to avoid interference with threat detection and blocking legitimate traffic.

- Address the inability to trace activity, recover clear-text information, and detect applications-level attacks (e.g., phishing attack based on a socially engineered email that contains a malware-infected PDF disguised as a corporate spreadsheet).

- Integrate with netflow and other diagnostics such as DNS intelligence, protocol patterns, netblock reputation, Web address reputation, IP address reputation, and country-of-origin information to reduce gaps in detecting malicious command-and-control systems.

- Supply updated behavioral rule sets to block further traffic associated with malicious sites and/or documents.

- Capture credentials "in the wild" from malware drop sites and other exfiltration rendezvous points that organizations themselves wouldn't have the ability to track down and recover.

The enterprise benefits of threat intelligence as a service are extensive. This is especially pertinent when enterprises consider the challenge of building/maintaining in-house real-time predictive security organizations and/or managing threats feed from many different security services. Overall, threat intelligence offers customers deeper insights into global threat environments than they could achieve themselves. Following are further advantages to threat intelligence as a service:

- Real-time threat intelligence data feeds and threat analysis updates customized to specific customer needs

- Deep search capabilities on threat indicators such as command-and-control protocols, IP addresses, malicious URLs, and DNS vectors

- Full-packet captures for analysis of network, host, applications, malicious file paths, and registry keys (In some cases, individual attackers can be finger printed, subsequently identified, tracked, investigated, possibly blocked, or routed to a honeypot/honeynet for further analysis.)

- Exploit details and execution traces captured for incidents, emergency response, and forensics

Market Overview

Threat Intelligence services vary in description and function. These services are delivered through cloud-based portals and data libraries that can be incorporated into existing enterprise threat management tools.

Threat intelligence services are typically sold the following ways:

- **Managed services,** including SaaS or cloud-based service delivery, where the systems are managed in the cloud or on the customer premise and are updated and managed with an advanced threat intelligence layer

- **Professional services,** revolving around security strategy and planning, analysis and review, and incident and emergency response activities

- **Data services,** which update managed devices under security service management with threat analysis and mitigation paths

- **Data feeds,** a differentiator for some vendors and are sold in raw form or increasingly as consumable threat intelligence, with analyzed data and remediation recommendations (Data feed services include threat intelligence and analysis that identifies threats and their severity, attack locations, behavior, geographical origins, reputation of source IP addresses, and relationship to known vulnerabilities. Services are typically offered on an annual basis with bundled subscriptions or licenses.)

Data feed suppliers can be segmented by their focus:

- Larger firms provide enterprise aggregation with internal and external sources. They focus on government accounts (Department of Defense [DoD] and criminal justice) in the United States and overseas.

- Some independent firms also supply data on an OEM basis for incorporation into security products and/or threat intelligence services. In fact, it is quite common for many threat intelligence firms to buy data feed from competitors and collaborators.

- There are also captive threat intelligence groups that are solely or largely focused on threat feed for their internal products and a few select customers and partners (often DoD and/or law enforcement). (The focus is largely on collaboration, not revenue generation.)

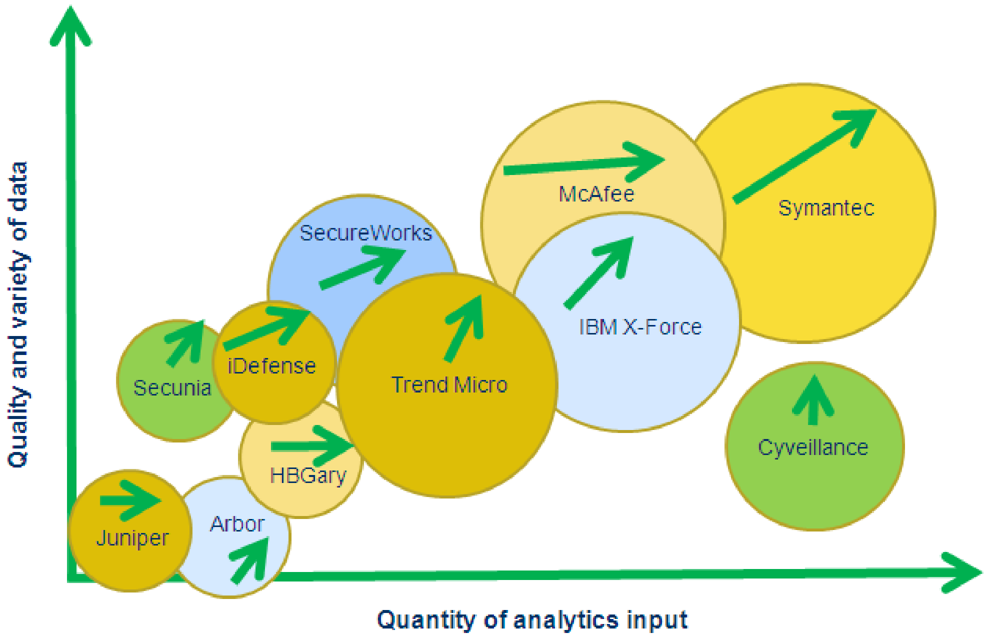
- Smaller firms specialize in threat-specific data feeds (e.g., Zeus, botnets, financial fraud, and retail fraud).

In practically all cases, these data feeds are based on analyzing large data flows (hundreds of thousands to billions of events per month), large databases of logs, authentication of sources, and global and country-specific data (especially from smaller, regional boutiques that may only support a few government and/or financial services customers).

Because the firms are so variable in this emerging threat intelligence markets, distinctions are difficult but apparent in the size and type of sensor networks, quality of heuristics engines, difference in analysis techniques, country versus region versus global focus, and the depth and experience of human analysis. As malware advances (communicating with command-and-control networks for validation, for example), established techniques will no longer be valid, and tomorrow those learned behaviors may not be true for long. Vendors will need to continually develop and innovate their techniques and methods for intelligence gathering and enrichment.

FIGURE 1

Security Services Threat Intelligence Solution Vendors' Competitive Positioning by Quality and Quantity of Threat Intelligence Data



Note: Arrows indicate future direction.

Source: IDC, 2011

IDC reviewed 11 vendors' threat intelligence solutions based on the criteria described previously; a summary of these individual vendors' threat intelligence solution profiles is provided (see Tables 1A and 1B). The following vendors were interviewed for this document: Dell SecureWorks, Symantec, Secunia, McAfee, IBM X-Force, Verisign iDefense, Arbor Networks, Juniper Networks, Cyveillance, Trend Micro, and HBGary. Following is a summary of these Symantec's' solutions:

- **Symantec DeepSight — Symantec Internet Security Threat Report, Symantec Intelligence Quarterly Report.** Symantec collects intelligence data from over 180 million endpoints and enterprise servers, as well as 240,000 network devices. The Symantec vulnerability analyst team aggregates and updates a collection of over 45,000 vulnerabilities covering 105,000 technologies. Symantec also analyzes daily over 8 billion emails for spam and phishing intelligence and over 1 billion Web requests. This data is collected globally from over 200 countries. This incredible data resource powers analytics that result in "predictive" threat identification capabilities that can be incorporated into security authentication functions. Rather than relying on traditional signature-based systems to identify possible threats, the predictive intelligence is used to create a reputation-based scoring model that is faster and more effective. DeepSight, the threat intelligence service offering from Symantec, combines worldwide threat data with proprietary and partner-provided security intelligence. The DeepSight service offers several service delivery options to incorporate threat intelligence and analytics into the security programs and processes enterprises use to protect against emerging threats. Clients can leverage DeepSight intelligence through the DeepSight Early Warning Services portal, which generates alerts when client-specified thresholds are met. Or by leveraging DeepSight DataFeeds, clients can integrate Symantec's intelligence directly into the enterprise applications they currently use to manage their security, risk, or governance programs through a data feed that consolidates threat, vulnerability, risk, fraud, spam, phishing, attacker, and network intelligence information and eliminates the problems associated with disparate threat sources.

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
Sensors	Gathers intel from more than 70,000 managed or monitored MSS devices around the world. CTU develops custom signatures for iSensor and Snort devices based on gathered intelligence.	Symantec collects data from 240,000 sensors and over 135 million endpoint products; this intelligence is passed directly into the Symantec Global Intelligence Network where members of the company's security teams analyze the data for malware, phishing, and other forms of attacker information.	27,000 products. 30,000 Secunia advisories. 12,000 file signature rules developed by Secunia. Unique nonintrusive scanners.	Gathers intel from 100 million McAfee product nodes. About half of those nodes (50 million) doing real-time querying. Look at info in passing.	IBM's threat intelligence is gathered not only from thousands of managed and monitored customer devices but also through global analytics tools, IP reputation tracking, sensor placement on darknets, data gathering from multiple honeypot nets and honeypots, and third-party external data feeds. IBM funnels a variety of this information into its X-Force Protection System (XPS), a cloud-based analytic engine and SIEM that provides advanced correlation and analysis and prioritization of suspicious behavior and attacks.	Verisign iDefense monitors 28,000 products from over 400 vendors. Capability to leverage the DNS backbone; visibility into 70 billion queries a day. Malware scans of 100+ million Web sites monthly. Visibility into DDoS attack activity/traffic for 100+ DDoS customers. Vast technical collection grid of 300+ open and closed data sources.
Human intelligence	Yes. More than 50 dedicated security researchers. There is also another team dedicated to operational intelligence.	Yes, more than 500 researchers analyzing intelligence for a variety of behavior types, as well as analyzing code for malicious activity.	Yes. Team of 10. Not looking at IP payload or text specifically, but vulnerabilities or proof of concept	350 researchers in McAfee Labs, Ph.D. and university level, focusing on statistical analysis, behavioral analysis, looking at all info that is anomalous.	Human intelligence in IBM comes from a variety of sources. Intel functions are divided into two main areas of responsibility: The X-Force R&D team focuses on strengthening the Tivoli product lines and maintains its worldwide threat intelligence capabilities. This team works across IBM to document and	iDefense human intelligence capabilities include more than 50 full-time dedicated intelligence analysts who speak over 20 languages and are subject matter experts in the areas of malicious code, vulnerabilities,

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
					analyze the current threat landscape and receives input from Managed Security Services, Professional Services, Emergency Response teams, and the Content Security Team, which monitors global Web crawler and international spam collectors. They also support the X-Force Database team, which catalogs, rates, and assesses threats in the world's largest threat data repository. The Cyber Threat Intelligence group is part of IBM's Managed Security Services line of business and leverages data from the MSS environment (4,000+ customers, 130+ countries, tens of billions of daily events) as well as X-Force R&D to create a regular flow of communication and analysis to X-Force Threat Analysis and MSS customer base.	threat actor reconnaissance, and geopolitical threats. iDefense's dedicated analyst team is extendible with a HUMINT network of over 600 security research contributors worldwide. These contributors provide iDefense with zero-day vulnerabilities as well as current intelligence on emerging regional security threats.
Government resources	Yes. Deep-seeded relationships with many three-letter agencies.	Yes	No. But cross-reference with national vulnerability database. Have customers in U.S. defense but nothing that limits it from disclosing	No	Yes. While many of these sources cannot be disclosed publicly, IBM is a member of the IT-ISAC and participates in information sharing efforts that include the Department of Homeland Security's U.S. CERT organization.	Yes

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
			vulnerabilities to the public.			
Honeypots (annual spend)	Yes	Yes. Symantec has an additional data source, known as AQS, which allows Symantec to deploy its own, plus partner with others to deploy honeypots that feed into its Global Intelligence Network.	No. Not feasible.	Hundreds of honeypots to augment threat intel.	The MSS Threat Intelligence Center manages a full class B darknet for monitoring as well as multiple honeypots that reside in that space.	Yes
Web crawling	Yes	Yes	Semi-automated: monitor bulletins, mailing list steam not looking at text specifically but vulnerabilities or provides a proof of concept.	Web categorization is its core competency for traditional threat detection. McAfee is one of three core vendors in that space. Knowing what sites are new, what sites are coming up on blacklists, gaining disposition, to see how it changes.	IBM has extensive Web crawling capabilities that index over 200 million unique pages per month. This effort feeds the world's largest filtering database containing over 10 billion evaluated Web pages. IBM's URL filtering list is also the world's largest at over 170 million cataloged and classified sites.	Yes. Verisign iDefense uses a variety of Web crawling techniques to support malicious code scanning of over 100 million sites, support IP reputation services, and provide advanced threat monitoring.
Other sources of telemetry data you capture?	IP and DNS reputation; open sources passive monitoring.	Symantec researchers use a variety of sources of intelligence for analysis of its	Rather than that Secunia validates what has been discussed out there (blogs, bulletins). Its	No	IBM gains tremendous insight from its purpose-built MSS infrastructure called the X-Force Protection System. It is a cloud-based analytic engine and SIEM.	Verisign iDefense captures and analyzes IP reputation and DNS data; open sources

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
Could be a byproduct of another?		Global Intelligence Network, from these sources Symantec catalogs and corroborates its internally gathered intelligence and uses this to create its various offerings in the intelligence space.	approach is to see errors that are being discussed in reports.		Through XPS, IBM provides sophisticated correlation and analysis across its MSS and third-party data sets, threading together sequences of activity that identify threats, automatically prioritizing the highest risk asset for remediation. The most recent enhancement to XPS includes real-time identification of direct attack, drive-by-download, and propagation or communication with botnet C&C feeds. Utilizing this interface, IBM automatically calculates the most active malware, the IDPS signatures that triggered and their geo-IP location, providing rich intel from which to triage the situation. Further, IBM leverages this system to generate industry and geocentric metrics for trending and baselining.	passive monitoring. DDoS attack monitoring.
Description of competitive security intelligence	Used for threat prevention since clients have limited resources. Looks for new threats, new attack vectors. Then integrates that threat intel into managed devices and host-based security controls. Also provides multiple deliverables to	Symantec provides customers with access to the company's processed and raw intelligence in the DeepSight Early Warning Services Portal as well as	Test and prove threat exploitability and advise users about vulnerabilities, and is free. Other companies track Secunia and see vulnerabilities and didn't report it and	Wikipedia of threat intel. Provides searchable info on threat intel for eight areas: application name, DNS server, intrusion attack, IP address, malware name, domain name,	IBM commercializes its security intelligence capabilities through its MSS business via its X-Force Threat Analysis Service, which provides daily analysis of the threat landscape and serves as a security newswire for dedicated subscribers and MSS clients. It also produces regular trend and	Verisign iDefense provides information security executives access to accurate and actionable cyberintelligence and decision support related to vulnerabilities,

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
	threat intelligence customers via the Web-based portal and email notifications. Includes CTU TIPS that provide immediate high-level information on new threats and vulnerabilities being researched or seen in the wild. Threat analyses are comprehensive reports on malware and emerging threats, and provide recommendations for identification and remediation. Microsoft Update Analyses provides threat intelligence customers with an in-depth look at all new Microsoft patch releases (within 24 hours) to assist in understanding and prioritizing patches. CTU support provides direct access to top researchers for security-related issues. Also full breadth of malware analysis and incident response services available.	its DeepSight DataFeeds products. These products allow end users to extend their intelligence gathering capabilities into the Symantec network and provide research tools as well as automated ingestions via XML. This gives clients the ability to not only research security incidents and events in its own portal but use its intelligence in their own networks to create meaningful correlations and contextual analysis of events that occur on their networks.	develop a patch and get it out.	Web site/URL address, vulnerability name.	threat reports throughout the year and leverages research capabilities to feed IPS attack signatures, content filtering modules, and the analytics engine behind its XPS back-end infrastructure. Last, IBM has the X-Force Database, which allows clients to search the world's largest repository of threat analysis and research.	malicious code, and global threats 24 hours a day, 7 days a week. Verisign iDefense in-depth analysis, insight, and response recommendations help keep enterprises and government organizations ahead of new and evolving threats and vulnerabilities. Over the past three years, the Verisign iDefense team has reported on over 10,000 vulnerabilities, including over 600 zero-day vulnerabilities, and provides vulnerability insights on average 180 days in advance of public disclosure by vendors.
Worldwide/ regional sensors	Worldwide	Worldwide	Worldwide	Worldwide	Worldwide	Worldwide
Portals	Yes. Robust portal	Yes, DeepSight	Yes	Yes	Yes. IBM provides a single	Yes, Verisign

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
	specifically for threat intelligence. Integrated with MSS portal but can be delivered to standalone TI customers as well.	Early Warning Services Portal (TMS). Provides clients with the ability to query Symantec's intelligence and create monitors that will inform them when any of a variety of actions are noted by Symantec analysts.			centralized vSOC Customer Portal for all managed security services and threat intelligence. In addition to reporting the information associated per service line, IBM consolidates this data via SIEM capabilities, offering full life-cycle capabilities for analysis, notification remediation, ticketing, and reporting.	iDefense customers have access to a deep portal for threat and vulnerability intelligence. It provides customers with the ability to schedule and deliver a variety of threat and vulnerability intelligence reports in multiple delivery formats. Automatic Malcode analysis via Verisign iDefense portal.
Data feeds: supply as raw feed? Feed with custom reporting? As both with dedicated analyst?	Several ways customers can consume the intelligence information: protections directly applied to managed devices and monitoring rule sets, email notifications, search, or browse through content in portal, and XML feeds.	Symantec DeepSight provides data feeds that can be leveraged by clients internally for use in whatever tools they may be using to create contextual analysis. In addition, relevant intelligence is provided to Symantec products, and continuous internal processes are in	Write up advisory and how vulnerability is triggered and spread and any other mitigation.	Either bundled as subscription or license. By subscription does A/V detection and file reputation. Web gateway is Web-based product on yearly basis.	IBM offers the X-Force Threat Analysis Service (XFTAS), which offers a comprehensive Web experience, customized alerting, API-based data feeds, and daily email alerts. The service is available for purchase standalone and is also bundled complimentary with all IBM Managed Security Services.	Verisign iDefense threat and vulnerability intelligence delivered as XML feeds via Web services. Verisign iDefense feeds can be easily integrated with existing security solutions including SIEM, MSSP, Vulnerability Scanners, Patch Management and other security solutions.

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
		place to determine whether new intelligence should be provided to Symantec product lines.				
Product integration — using source of intel and methods of dissemination	MSS and TI clients get updates from CTU and SOC with SLAs on how quickly they publish a vulnerability once discovered. CTU writes custom signatures and correlation rules for MSS. Customer advisories published to inform of emerging threats that are likely to impact their environment.	Integrated into many Symantec products, as well as dissemination via the DeepSight intelligence products.	SaaS delivery model; products and free consumer software of updates based on teams' research.	Integrated across 13 product families, which is double than last year. Now represents over 90% of McAfee's GTI business.	Threat Intelligence is diverse and bidirectional across the IBM product and services teams. Raw MSS data, for example, fuels correlation and automated threat analysis that is used by both products and services. For example, this raw data is sent to the X-Force R&D team to consolidate with their own data sets to perform additional analysis that fuels enhancements to the Proventia Product Line and into the X-Force Threat Analysis Service.	Verisign iDefense intelligence is integrated into many products such as Qualys, HP ArcSight, RSA Archer, RSA NetWitness, Agiliance, and Skybox.
Customer segmentation	More than 250 threat intelligence customers. Most are also MSS customers, though several are not. Customer breakdown by industry: manufacturing — 10%; technology providers — 10%; utilities — 10%.	Symantec's DeepSight clients run the range of industries and customer sizes. Symantec's packaging of these intelligence services provides an option that is designed to fit any clients' needs.	Only industry player targeting both B2B and B2C on VM. Global 2000; DACH, Nordics, North America, and the United Kingdom. B2B — large accounts, enterprises, and SME's strategic accounts. B2C —	At best, McAfee was looking at log info and traditional SIEM information after the fact and looking at event correlation and can see it as it's happening. Provides McAfee a new way to makes sales.	IBM targets midmarket to large enterprise and focuses cross-industry. Key sectors include financial services, healthcare, energy and utility, and retail and distribution. Unique capabilities support customers with varying needs such as base subscription threat analysis service, a redistribution license for customers looking to do more with data feeds, and optional	Verisign iDefense serves a large and diverse customer base. Customer count segmentation by vertical: financial services 45%, technology 16%, public sector 14%, energy/utility 5%, retail 5%, and HLS 3%.

TABLE 1A

Security Services Threat Intelligence Solution Profiles by Vendor

Questions	Dell SecureWorks	Symantec	Secunia	McAfee	IBM X-Force	Verisign iDefense
			security aware and "well educated" users. Statistics: 5 million unique users. PSI installations: 2+ million. Enterprise customers: 1,042.		Security Intelligence Analysts who remotely work with the customers to serve as an extension of the customer's security team.	

Source: IDC, 2011

FUTURE OUTLOOK

Forecast and Assumptions

IDC forecasts the security services threat intelligence market to reach almost $800 million in 2013 and growing to $905 million by 2014. The CAGR for 2009 to 2014 is 35.5% and spans large, medium-sized, and small businesses, with large businesses showing the largest CAGR at 48.9% over that same time period. We based the forecast on enterprises currently comfortable with outsourcing their network, application, and endpoint security event monitoring but have an understandable reluctance to allow blocking or remediation of those security events. It will take four to five years to complete the migration of intelligence services from raw data streams to proactive information available in a variety of forms across multiple channels. See Table 4 for top 3 assumptions and Table 5 for key forecast assumptions underlying the worldwide and U.S. security services threat intelligence 2011–2014 forecast.

ESSENTIAL GUIDANCE

Threat intelligence products and services are increasingly being adopted by the commercial sector as APTs, zero-day attacks from hacktivists, and cybercriminal activity awareness are growing. The APT conundrum is that signature-based security products are ineffective against APTs, but it creates opportunities for threat intelligence and predictive security services. Following are some trends IDC sees happening in the threat intelligence market:

- Previously, just government, very large enterprises, and financial services were the object of targeted attacks due to higher payloads for cybercriminals from these targets. The commercial sector has read about the high-profile data breaches and the subsequent brand degradation and regulatory compliance problems they've caused and are also aware of the security risk. That is leading to more services being created by security services vendors to thwart those attacks and increased adoption for those services. A global service firm recently said, "We don't want reactive or even the current, so-called proactive security stuff. We want predictions for unknown and previously unseen threats. We want actionable solutions BEFORE the problems occur." If vendors make services more packaged for repeatable sales, that would make it a lot more available and accessible to a lot more people.

- Signature-based tools (antivirus, firewalls, and intrusion prevention)_are only effective against 30–50% of current security threats. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly. Enterprise customers loudly complain that installed signature-based products (antivirus, firewalls, and intrusion prevention) are useless against targeted zero-day attacks and APTs. Enterprises want data sources that will help them predict new attacks. "We are getting hammered by malware that is circumventing signature-based security products. We need actionable recommendations," according to a large financial services firm.

- Telco, SI, and pure-play security services vendors are making partnerships and acquisitions and building threat intelligence information services. Prescriptive recommendations are becoming more common to help less experienced customers benefit from threat intelligence services. Over time, threat intelligence services will become more targeted for nontechnical customers. Adding actionable intelligence to the data is the big opportunity for SMB customers and software vendors that want to "bake" proactive security intelligence into their system, network, storage, and desktop management products and services. Integrate data feeds with security and vulnerability management, SaaS, and other products for protection against advance persistent threats. Package as SaaS and consulting services. Enterprises will look for partnerships such as VeriSign's iDefense and/or vendors like Secunia that do vulnerability assessments and clearly demonstrate vulnerabilities to the endpoint.

- Product vendors are coming to market with products so services wrapped around this area could have strong traction. Examples include appliances that automatically detect malicious PDF files, botnets, and other stealth espionage at the perimeter using behavior-based method for detecting targeted, non-signature-based malware; capturing executable code within the operating system; and unauthorized running of programs that can be found in physical memory, including targeted attacks, rootkits, injected code, and custom malware.

- Many small consulting firms worldwide monitor traffic for specific client requirements, by purchasing feeds and monitoring public data and by developing relationships with local and state governments within those countries for command-and-control access. Small and medium-sized threat intelligence vendors will find it increasingly difficult to process huge volume of incidents, so smaller vendors will specialize on specific threats, verticals, country/regional issues, analysis, and remediation. Consolidate midtier and small threat intelligence feeds.

- The public sector is very mature and sees attacks earlier than the private sector but do not have access to as much data as Symantec or Google. The value-add is providing access to unique information and security analysts that can interpret that data for the public sector. Commercial sector opportunity revolves around providing actionable intelligence attack actors and techniques used against the public sector after they are no longer effective against the public sector. SYMC can bridge the gap between public and commercial since some zero-day findings cannot be shared, depending on the source of intelligence. In response, the DoD is expanding its Contractor Cybersecurity Program. This is a pilot program that shares threat information with defense contractors and network providers and has stopped hundreds of intrusions.

- Intersection of data (public and commercial), volume of data, requirement for interpretation, and value-added services are a unique combination that practically all CSOs are interested in discussing. Many vendors in this space bridge public sector, law enforcement, and commercial sources for their threat intelligence services as command-and-control data from these sources provide rich information.

- Only a small percentage of public and private sector customers were doing their own threat detection with dedicated staff, honeypot nets, and their own data feeds. Most IT organization data is from external, independent organizations. Technical personnel are required for vendors providing threat intelligence services and customers doing threat intelligence in-house. These highly skilled workers are scarce, with 0% unemployment for IT security personnel. Technical personnel are required for vendors providing threat intelligence services and customers doing threat intelligence in-house. Advanced computer science degrees bolstered by a minimum of two to three years' research or managed security services experience is required to evaluate and utilize threat intelligence. On a worldwide basis, a very very small number of enterprises could make this work and effectively incorporate a variety of issues: political issues (like privacy, data retention, law enforcement, etc.), manage data collection (logman, SIEM, and analysis), and run a profitable business.

- Be aware of backlash against "Big Brother" intrusion and monitoring methods. Cyveillance recently suffered some bad press for monitoring chat rooms and other data communication that some would consider private, all in the name of protecting its customers' intellectual property. But the presence of a monitoring agent that logs everything, then stores it in a database, and maybe even selling that data to another corporation or government concerns many people for a number of reasons.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.