WHITE PAPER:
SYMANTEC GLOBAL INTELLIGENCE NETWORK
2.0 ARCHITECTURE

Symantec™ Global Intelligence Network 2.0 Architecture: Staying Ahead of the Evolving Threat Landscape

Who should read this paper

Information Security executives and teams can use this document to understand new improvements made to Symantec's Global Intelligence Network.

Confidence in a connected world.

Symantec™ Global Intelligence Network 2.0 Architecture: Staying Ahead of the Evolving Threat Landscape

Content

Staying Ahead of Threats

The threat landscape not only continues to become more hostile, but it changes and evolves at a dramatic rate that makes it increasingly more difficult for security professionals to stay ahead of the threat curve. The volume of attacks continues to rise as do the variety and sophisticated nature of attacks. This requires organizations to take a more intelligent approach to protecting and securing their infrastructure.

In the face of such a dynamic and sophisticated threat environment, security professionals need answers to vital questions. How can they proactively address so many potential threats coming from so many different directions and venues? How can they quickly close critical vulnerabilities given personnel, budget and time constraints? What can they do to protect against targeted attacks? How can they detect stealth and morph attacks? Given their existing limited resources, how can they minimize the impact of the growing range of malware? How can they succeed against seemingly unlimited resources from malicious nation states, cyber terrorists, and organized professional cybercriminals? How can they predict, prepare and respond to the innovative variety and escalating volume of sophisticated threats and attacks?

The answer to these questions lies in greater security intelligence. Quality security intelligence gives security professionals and organizations a greater understanding of the threat landscape, the threat actors launching those threats, and the way that many seemingly different and disparate threat activities are actually tied together. But with the sophistication and constant evolution of the threat landscape, security intelligence itself must also evolve. A much broader stroke must be taken in terms of gathering security intelligence across the entire depth and breadth of the threat landscape. That broad spectrum of security intelligence must be able to be fused together, refined and analyzed in a way that it can then be delivered in a manner that provides easily consumable, actionable and customized security intelligence—security intelligence that allows organizations to proactively predict, identify, prioritize, and rapidly mitigate threats. The next generation of the Symantec Global Intelligence Network (GIN) is the embodiment of this new evolution in security intelligence.

Advantages and Evolution of Security Intelligence

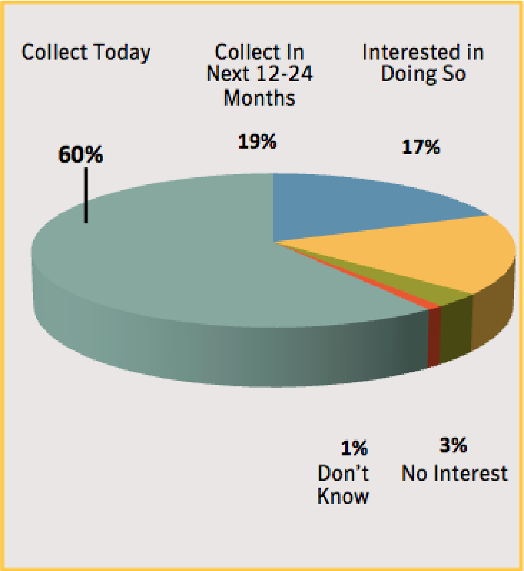
Intelligence driven security enables organizations to respond more effectively to the vast array of new and evolving sophisticated threats. It gives organizations the advantage of making more informed security decisions and responses. Intelligence driven security empowers security professionals to prioritize and focus on the most pertinent threats and vulnerabilities to engage in more proactive actions with greater efficiency and speed. Security intelligence also opens the door to providing organizations with new forms of protection that better equip them to address the wide array of new and emerging threats.

It's no wonder that the demand by organizations for greater security intelligence continues to rise. The IDC Security Services Threat Intelligence 2011-2014 Forecast shows that organizational investments in security intelligence solutions grow at about 35 percent a year. The ESG 2012 Security Analytics Study reports that of the 249 large enterprises that it surveyed, 60 percent currently acquire and use security intelligence as part of their security strategy and that 19 percent plan to in the next 12 to 24 months. Additionally, the ESG study found that of those enterprises with a mature security program, all of them acknowledged the effectiveness of security intelligence, while 57 percent praised security intelligence as being highly effective.

Security Intelligence Facts

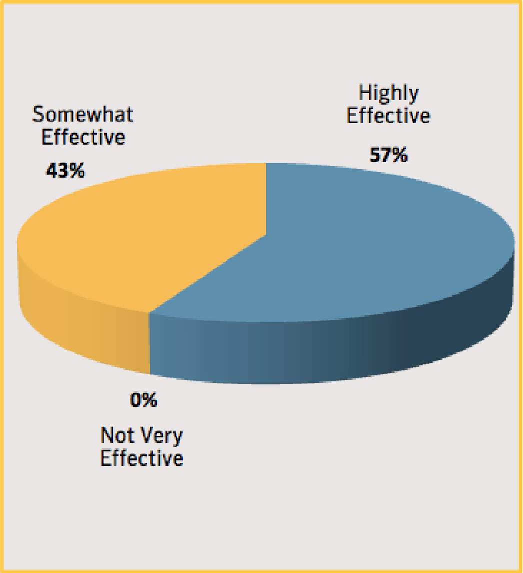
- Security intelligence investments grow annually by 35 percent (IDC)
- 60 percent of large enterprises leverage security intelligence, 19 percent plan to within the next 2 years (ESG)
- 100 percent of mature security intelligence users affirm its effectiveness, 57 percent cite it as highly effective

% Enterprises Collecting External Threat Intelligence Data



Source: ESG 2012 Security Analytics Study

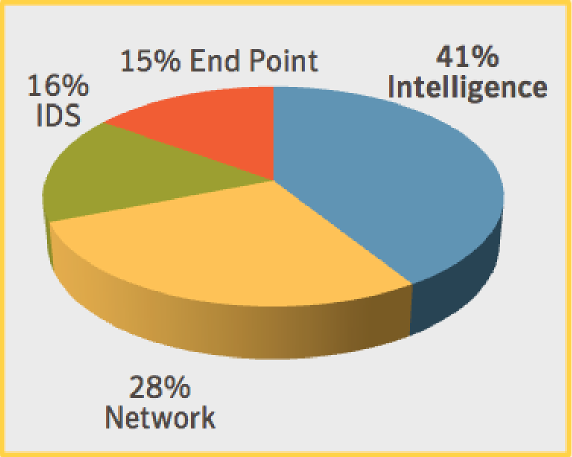
Effectiveness of Threat Intelligence in Advanced Users



Source: ESG 2012 Security Analytics Study

From its own experience through the managed security service Symantec provides to enterprises, it found that 41 percent of severe threats to customer infrastructures were detected through security intelligence. Standard security solutions, such as network security systems, intrusion detection and prevention systems, and endpoint security solutions detected the other 59 percent. For organizations that do not leverage security intelligence, this translates into a significant number of severe threats that can potentially go undetected.

Symantec Security Intelligence Proven Highly Effective in Detecting Severe Incidents



In spite of the significant advantages and effectiveness that security intelligence provides, it too needs to evolve in order to stay ahead of the ever-changing and growing threat curve. The constant and dramatic increase in the volume of attacks calls for substantially more security sensors for gathering security and threat data. The broader array of differing forms of attack requires different types of sensors and different ways of acquiring intelligence. As the types of attacks continue to change, new ways of detecting these attacks need to be introduced.

Additionally, such advances in security intelligence create challenges in handling the massive volume increase in acquired threat data, including resolving issues with complexity and speed of data analysis, and the delivery and consumption of the resulting security intelligence. To deliver on all these security intelligence advances and address their associated challenges, Symantec has unveiled the next generation of its highly touted security intelligence platform, Symantec Global Intelligence Network.

Greater Depth, Breadth and Quality of Security Intelligence

Symantec developed the first iteration of its Global Intelligence Network as a vast network of data collection sensors for gathering and collating data on security incidents, events, and vulnerabilities around the world. It has become the nucleus of Symantec's security intelligence capability, not only powering the wide variety of Symantec security solutions, but positioning Symantec as the leading provider of security intelligence to enterprises globally. As a result, IDC has recognized Symantec as the leader in security intelligence services with the highest quality, most accurate, and widest variety of security data than any other major security vendor.[1]

As such, Symantec is uniquely positioned among security vendors to enable organizations to stay ahead of the rapid evolution and expansion of the threat landscape. With this objective in mind, it has redesigned and rebuilt its security intelligence network from the ground up to enable Symantec to collect even more threat data from more data sources, correlate that data more accurately, and deliver more reliable analyses and conclusions even faster.

Symantec Global Intelligence Network provides an expanded range of even higher quality security intelligence that enables organizations to:

- Make more proactive and intelligent decisions on where to allocate and focus resources
- Make more proactive and intelligent decisions on what actions to take to minimize risk
- Respond quicker to the most significant and relevant threats
- Remediate and recover from incidents faster
- More efficiently, effectively and proactively secure their infrastructures against the escalating variety and volume of sophisticated cyber threats

Next Generation Security Intelligence Revealed

This next generation of Symantec Global Intelligence Network introduces new data fusion techniques that enable the analysis of a significantly broader set of data from the cyber-threat landscape and has the ability to quickly transform that data into more meaningful, actionable and consumable security intelligence. The next-generation GIN is comprised of the following main architectural elements:

- Expanded Sensor Network
- Big Data Security Platform and Warehouse
- Multi-Level Trust Model
- Unified Security Intelligence Data Model
- Fusion Analytics Engine

[1]- IDC: “Worldwide and U.S. Security Services Threat Intelligence 2011-2014 Forecast: Out of the Basement and into the Clouds,” http://idcdocserv.com/230490E.

Expanded Sensor Network

The increases in attack volume, the wide array of different attack methods, and the rising connection between attacks across the threat spectrum demand a global approach to gathering data on security and threat events. Even though Symantec already had the largest and most extensive security intelligence network among all security vendors, it recognized the need to do even more in response to the rapid evolution of the threat landscape.

Symantec Global Intelligence Network next-generation facts:

- Global sensor network expanded by 2,216 percent
- Analyzes 44 percent more event data
- Typical analytics query time decreased by 99.3 percent

With the release of the next generation of Symantec Global Intelligence Network, Symantec has expanded its global sensor network by 2,216 percent. This expansion drastically increases the range and amount of threat activity that it collects from its sensors, giving Symantec a significantly broader view and deeper insight into the entire threat landscape. When combined with other new functionality built into the next generation of GIN, this expansion leads to a significant augmentation to the overall quality and reliability of Symantec's security intelligence.

But Symantec isn't done growing its network of threat sensors. With the vastness of the Internet and its constant growth, it is only possible to see a limited percentage of the activity that takes place. For this reason, Symantec continues to constantly look for new geographical locations and threat areas where it can establish new sensors for its global network.

To make it easy to roll out new sensors quickly and easily, Symantec employs an extremely flexible sensor model. A considerable number of the intelligence network's sensors are deployed as part of products and services that Symantec provides Fortune 100 companies and other large enterprises. Others come from third-parties and Symantec customers. This allows sensors to enjoy broad distribution as well as take on a wide variety of forms, including different types of security devices and software such as network gateways, cloud security, enterprise grade endpoint protection software, and even consumer oriented antivirus software.

Adding to the broader view that the next generation of the Symantec Global Intelligence Network provides, the expanded sensor network gathers security data across the following four major threat landscape areas:

- Malware
- Fraud (for example spam and phishing)
- Software and hardware vulnerabilities
- Network based attacks

Instead of only mining individual threat areas like most security vendors, gathering data across all these areas and then fusing that data together with its analytics processes gives Symantec the ability to present a larger and more granular view of the entire threat landscape.

In addition to its automated sensors, Symantec employs security analysts around the world to manually gather security intelligence. These analysts study new threats and vulnerabilities from a variety of sources, and then feed that intelligence into the Symantec Global Intelligence Network.

Big Data Security Platform and Warehouse

With the massive expansion of the number and types of sensors in Symantec Global Intelligence Network, Symantec now collects more data about more security incidents and more information about each individual security incident. This has already led to a 44 percent increase in the amount of data collected and stored each day, and it's expected that the data volume will continue to increase.

This required increase in the flow of data into the system drove the need for Symantec to entirely rebuild its GIN architecture upon a big data computing platform with a big data warehouse specific to the needs of security intelligence data. Moving the architecture into the realm of big data empowers Symantec to scale its security intelligence capabilities as needed now and in the future.

This new computing platform and security data warehouse gives Symantec the processing power and storage resources needed to gather this immense amount of data, logically link and fuse it together, and analyze it in a way that results in an extremely higher quality of security intelligence. In fact, this new computing platform has decreased the time a typical analytics query takes by 99.3 percent. This significant increase in how fast the platform can calculate and act on data is essential to its ability to perform complex analyses across large volumes of data in real-time.

By redesigning and re-building the Symantec Global Intelligence Network to leverage a big data computing platform and security data warehouse it can:

- Continually scale its ability to gather extensive security data across numerous sources
- Maintain extensive histories on security activities and incidents
- Rapidly manipulate, analyze and deliver big data security intelligence
- Provide customers more information about relevant threat incidents; how they behave and why, and how to more easily protect and remediate against them

Multi-Level Trust Model

The Symantec Global Intelligence Network maintains and utilizes a multi-level trust model that allows it to reliably determine the confidence level of reported events. It's expected that when dealing with global networks of more than 64.6 million sensors across more than 200 countries and territories, that not all sensors will report events with the same level of reliability. To ensure the highest quality level of its security intelligence, GIN tracks the quality and reliability of each individual sensor and each sensor network at different sites and regions. This allows GIN to place a confidence rating on reported events based on the track record of the sensor or sensors that reported it. Events from more reliable sensors will be weighted with higher confidence than events reported by less reliable sensors. By employing this multi-level trust model, security professionals can make more insightful and intelligent decisions regarding the urgency and relevancy of potential threats.

Unified Security Intelligence Model

The new unified security intelligence model in Symantec Global Intelligence Network integrates data collected from different sources into a common security data model that eliminates inconsistencies and duplication of data. It maps data representing different event types into specific activity categories, recording specific event attributes, such as the attacker, nature of the event, vulnerabilities, cause, payload files, geographic location, source identification and more.

For example, when it collects information on an event, it records the attacker, details of the event type (for example phishing), the geographic location where the attack took place, the cause of the attack (for example attached document), whether the attack was launched against a specific vulnerability in a specific piece of software, and other descriptive information. With these event attributes of different event types stored in a common model, the analytic processes in GIN can more intelligently weigh the threat level and maliciousness of certain events, as well as detect patterns and connections between disparate events.

In essence, the unified security intelligence model blends data and provides filtered intelligence that facilitates the ability of the Symantec Global Intelligence Network to quickly and accurately analyze data from a wide variety of different sensor types on a wide variety of different threat activity. This filtered intelligence and blending of data into a standard model provides the basis for establishing quality metrics, while further increasing the scalability and speed of accurate analysis for the extensive depth and breadth of security intelligence provided by GIN.

Fusion Analytics Engine

The new fusion analytics engine in Symantec Global Intelligence Network is essentially a sophisticated analytics engine. After the unified security intelligence model performs its data integration and intelligence filtering, GIN stores that data into a standardized fast query database. Once in the database, the fusion analytics engine performs queries that correlate, sort, combine and slice data in a variety of ways to identify relationships between threat events and to create various threat projections.

Fundamentally, the fusion analytics engine asks different questions of all the data across all the different threat categories. These questions might include, what types of events are we seeing? Where are these events occurring? How many places are we seeing these events? What time did these events occur? How often are we seeing them? What's the relative maliciousness of these events? How confident are we in the reports on these events?

It's important to note that this process is a significant departure from traditional data security analysis. While the GIN fusion analytics engine asks these questions against all the data across all threat categories, most security solutions only ask questions of a data set within a single threat category. Security intelligence isolated to only one or two threat categories doesn't tell the complete story of the potential threat.

One of the most perilous aspects of today's threat landscape is that professional cybercriminals launch sophisticated attacks that employ and intertwine attack methods and vectors across multiple threat categories. A spam campaign might be tied to a phishing campaign, which might have links to certain malware code. By querying the totality of the data collected across all threat categories, the fusion analytics engine provides insights into the full scope of even the most sophisticated threat campaigns. This is key to generating security intelligence that gives organizations a greater understanding of the entire threat landscape, its threat perpetuators and threat trends, so security professionals can better protect and secure their infrastructures.

More Accessible, Consumable and Flexible Security Intelligence

Perhaps the most powerful aspect of the Symantec Global Intelligence Network is that it empowers organizations to move beyond basic incident response into proactively predicting and managing risk. Security professionals, IT managers and other consumers of security intelligence can leverage the information in GIN's data warehouse through a comprehensive array of customizable platforms and services. GIN makes it easy for organizations to consume, leverage, and act on its security intelligence in a way that makes the most sense for their unique business and infrastructure security needs.

The following represent the main delivery and usage models provided by Symantec Global Intelligence Network:

- Hosted security intelligence with Web portal
- Real-time automated security data feeds
- Embedded intelligence within Symantec security solutions
- Embedded intelligence within third-party security solutions

The variety and flexibility of its delivery and usage model eliminates the one size fits all model for security intelligence. The Symantec Global Intelligence Network offers a more personalized approach to providing the security intelligence that organizations need.

Embedded Intelligence within Symantec Security Solutions

To make it even easier for Symantec customers to take advantage of the benefits offered by Symantec Global Intelligence Network, an increasing number of solutions in the Symantec security portfolio automatically leverage GIN's security intelligence. From executive dashboards to event management consoles and more, these solutions transparently embed some or all of the Symantec™ DeepSight Intelligence DataFeeds to proactively protect against and respond to threats.

Embedded Intelligence within Third-Party Security Solutions

In addition to its own off-the-shelf offerings, Symantec enables other organizations and third-party security vendors to take advantage of the vast security intelligence provided by Symantec Global Intelligence Network by enabling them to also embed its data feeds into third-party solutions that might already be deployed in a customer network. Through the use of a Web services API, these providers can subscribe to and transparently integrate with any of the Symantec DeepSight Intelligence DataFeeds.

More Proactive, Faster and Intelligent Threat Protection

The Symantec Global Intelligence Network is the largest and most sophisticated security intelligence network in the world. Its ability to fuse the analysis of malicious activity across the entire threat landscape provides organizations with more intelligent insight than any competing offering, and provides it faster and in greater depth. Whether through integration with security solutions or through Symantec DeepSight intelligence services, GIN is in the distinctive position of being able to deliver the highest quality intelligence when organizations need it, empowering them to make better decisions, act faster, and be more effective in reducing their overall risk so they can stay ahead of the evolving threat landscape.

To learn more about the next generation of the Symantec Global Intelligence Network and associated Symantec intelligence driven security offerings, contact your local sales representative.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com