A CyberEdge Group White Paper

Licensed by Webroot

June 2014

SELECTING THE RIGHT THREAT INTELLIGENCE OEM PARTNER

Licensed by:

WEBROOT
BrightCloud® Security Services

CYBEREDGE
GROUP

EXECUTIVE SUMMARY

Your security products may feature the fastest detection engines, the most comprehensive feature sets, and the best user interfaces that money can buy, but if their cyberthreat intelligence feeds are not up to snuff, then you might as well pack up and go home.

We live in a world where cyberthreats are highly targeted, short-lived, and growing exponentially. Beyond traditional PCs and laptops, mobile devices are now in the crosshairs of cybercriminals and state-sponsored threat actors. Without highly accurate and actionable threat intelligence, your customers are loading their cyberthreat weapons with blanks.

There are numerous challenges facing information security vendors today—especially for vendors competing against the 'big boys' with armies of security researchers and massive threat intelligence networks. For one, it's challenging enough to find one threat intelligence OEM vendor with a broad portfolio of Internet, file, and mobile threat intelligence feeds. But even if you locate such a vendor, you must ensure their intelligence feeds are constantly updated, highly accurate, span a large geographic reach, and—equally as important—they must be easy to integrate into your own product offerings.

The purpose of this white paper is to describe threat intelligence feeds commonly licensed by security vendors and to educate you about what to look for—and, more importantly, what to avoid—when evaluating potential OEM partners.

EVOLVING MARKET INFLUENCES

Before we explore common threat intelligence feeds and the challenges security vendors face when integrating them, let's quickly recap a few trends that have emerged over the past half-decade that have monumentally impacted the way that security products must operate to defend networks against data breaches.

THREATS ARE HIGHLY TARGETED

Advanced cyberthreats facing enterprises and government agencies are highly targeted. Hackers leverage social media sites, such as Facebook and LinkedIn, to customize spear phishing emails that pose as legitimate messages from trusted friends and colleagues.

Malware associated with these advanced threats is highly customized, as well. Whether malware is designed to exploit known OS or application vulnerabilities using an off-the-shelf exploit kit, or whether it's designed to exploit an unknown vulnerability associated with a zero-day attack, many of today's advanced threats sail past traditional signature-based endpoint and network security platforms as if they weren't even there.

Even the latest sandboxing malware analysis platforms aren't foolproof. Threats may be hand-carried into the office on mobile devices thus bypassing your perimeter sandboxing defenses, or sometimes malware is designed to evade sandboxing platforms altogether by suppressing its malicious payload for a short period of time or until a certain action is performed by the user (i.e., scrolling down to page five of a PDF).

MALWARE IS GROWING EXPONENTIALLY

Numerous information security vendors publish statistics on the growth of malware from month-to-month and/or year-to-year. Although statistics vary with each researcher, it's clear that instances of reported malware is consistently on the rise and is growing exponentially.

In the first half of 2014, the AV-TEST Institute alone registered an average of 220,000 new pieces of malware per day (see Figure 1). That's up from 182,000 in 2013 and 100,000 in 2012. That equates to over 9,000 new malware samples per hour, over 150 per minute, and more than two malware samples per second!

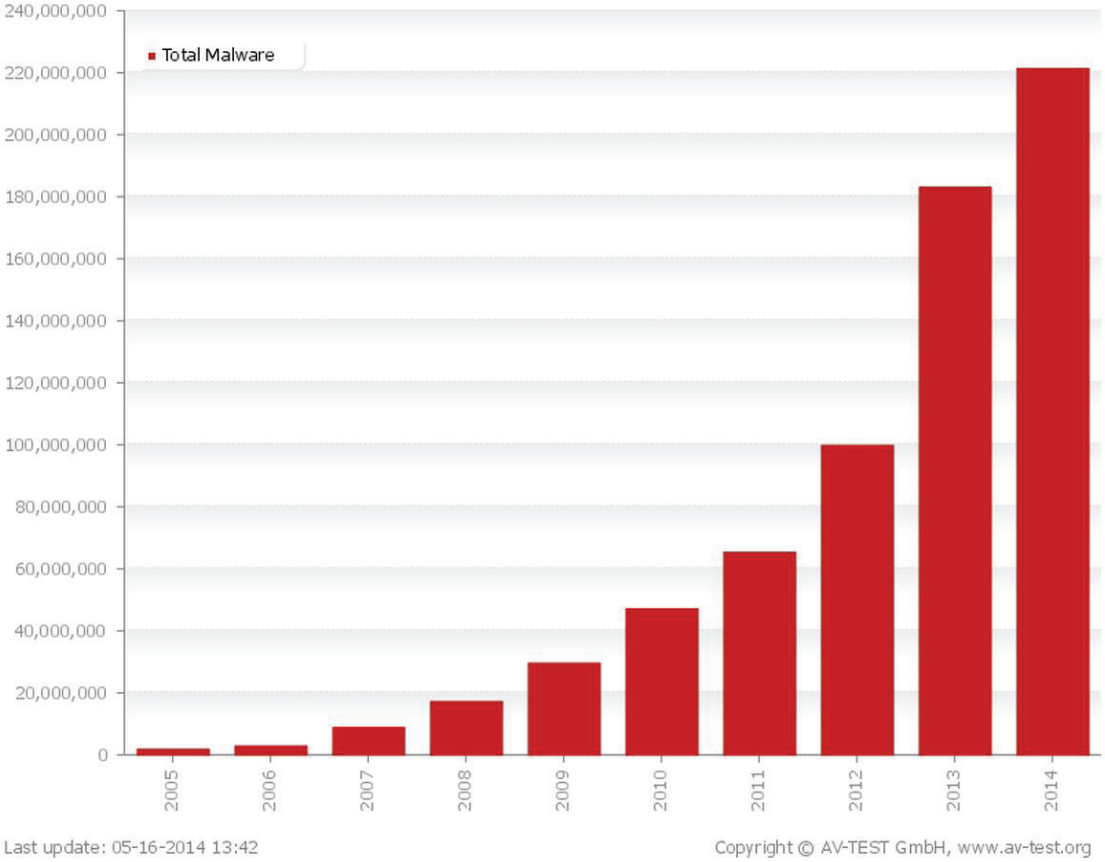


Figure 1: Average malware samples registered per day by AV-Test Institute (2005-2014)

MALICIOUS SITES ARE SHORT-LIVED

Malicious websites that host malware associated with spear phishing campaigns, waterhole attacks, botnets, and advanced persistent threats (APTs) are often short-lived. According to a security industry non-profit called AntiPhishing Working Group (antiphishing.org), the average life span of a phishing site is just 54 hours! A website URL one day may be deemed safe, but the next day be deemed malicious. In fact, it's not uncommon for these sites to be online for a matter of days or even hours before they're taken down and pushed live to another IP address or domain name. Security products that update their reputation feeds only once or twice per week are particularly vulnerable to savvy attackers.

MOBILE THREATS ARE ON THE RISE

Adoption of bring-your-own-device (BYOD) policies that enable workers to use personally owned tablets and mobile phones to access corporate applications and data has fueled a massive spike in mobile threats—especially against Android and iOS devices. In fact, information security vendor, Webroot, found that 28% of Android apps it analyzed in 2013 were malicious or potentially unwanted, which is more than double the percentage in 2012.

COMMON THREAT INTELLIGENCE SERVICES

There are a myriad of ways for malware to penetrate company-owned endpoints and network security defenses. The best strategy for mitigating cyberthreats, as always, is 'defense-in-depth.' Of course, a defense-in-depth strategy is only as good as the threat intelligence built into its layers of defenses.

This section explores common threat intelligence services divided into three categories—Internet, file, and mobile.

INTERNET THREAT INTELLIGENCE

Internet threat intelligence services correspond to security products designed to mitigate threats associated with web browsing and email.

- **Web classification/reputation.** Web classification threat feeds categorize hundreds of millions of URLs into categories enabling security products designed to filter safe/approved URLs so employees cannot connect to malicious (i.e., malware-infected) and/or inappropriate (e.g., pornography, gambling) websites. Web reputation threat feeds assign a score from 1 to 100 to each URL enabling organizations to finely tune their web security settings to proactively limit the risk of end user exposure to malicious web content.
- **IP reputation.** Modern hackers employ multiple techniques to hide their identities and activities, such as encrypted communications, DNS cache poisoning, URL redirection, hyperlink obfuscation, and more. IP reputation feeds enable security products to block (or alert on) all communications associated with known-bad IP addresses associated with malicious Internet hosts.
- **Anti-phishing.** New websites associated with phishing and spear phishing attacks pop up virtually every minute of the day. An anti-phishing threat feed—when updated in real time throughout the day—enables security products to block (or alert on) malicious Internet traffic associated with phishing and spear phishing attacks by evaluating a variety of factors, including web classification/reputation, IP reputation, how long the site has been in existence, recent threat history, and more.

FILE THREAT INTELLIGENCE

Virtually every major data breach in recent years—including Target, eBay, Adobe, and Heartland Payment systems—was caused by the download of a malware-embedded file (e.g., Adobe PDF, Excel spreadsheet) through some social engineering attack (usually spear phishing). Many of these attacks could have been avoided through modern file threat analysis solutions.

However, in order for such a solution to function optimally, it must be equipped with up-to-the-minute file threat intelligence. Such intelligence enables the security product to uniquely identify malicious files of all types, regardless of filename, platform, encryption or password protection.

MOBILE THREAT INTELLIGENCE

Implementation of BYOD policies by corporations is both a blessing and a curse. Financial gains resulting from improved employee productivity and job satisfaction can be offset by increased IT security risks. Two mobile threat intelligence feeds are critical for security products designed to mitigate mobile threats:

- **Mobile app reputation.** Helps organizations with mobile security products restrict tablet and smartphone apps based on the organization's risk tolerance. Mobile apps are evaluated and categorized into a multi-tier classification structure. Mobile app blacklists are typically updated on a daily basis.
- **Mobile security.** Mobile security intelligence typically features antivirus, antimalware, device and application interrogation, secure web browsing and classification, and an overall device score for administrators to assess the risk levels of devices on their network.

TYPICAL THREAT INTELLIGENCE LICENSING CHALLENGES

Security vendor product managers and engineers essentially have three choices for obtaining threat intelligence for their company's security products:

- **Option #1 – Build threat intelligence infrastructure.** Security vendors are certainly free to build out their own threat intelligence infrastructure just as many of the billion dollar security players have done. However, for most vendors, it's simply not practical to reinvent the wheel. The capital costs and personnel required to launch and maintain a global threat intelligence infrastructure is simply unsustainable. Plus, your security products require comprehensive, real-time threat intelligence on day one.
- **Option #2 – Leverage open source and/or crowd-sourced projects.** Some security vendors incorporate regurgitated, publicly available threat intelligence made available for free by open source and/or crowd-sourced projects. Although 'free' sounds compelling, when it comes to threat intelligence, the old adage applies—you get what you pay for. Threat intelligence from such projects is typically outdated and is much more prone to false positives and false negatives than threat intelligence sourced from reputable vendors.
- **Option #3 – License threat intelligence from a reputable vendor.** Most successful security vendors—especially those in the top-right 'Leaders' box of Gartner Magic Quadrants—license threat intelligence from one or more reputable vendors. Such vendors offer broad service portfolios and are accustomed to working with best-of-breed security vendors.

Option #3 is the obvious choice for most security vendors. Unfortunately, evaluating threat intelligence providers is not as easy as it seems. No two providers are alike and the quality of threat intelligence varies widely. This section describes typical challenges that security vendors often face when acquiring threat intelligence services from less reputable sources.

SOURCING DISPARATE THREAT INTELLIGENCE SOURCES

Rarely does a single security product incorporate just one type of threat intelligence. A typical secure web gateway, for example, is equipped with threat intelligence derived from a web classification feed, a web reputation feed, an IP reputation feed, and perhaps even a file threat intelligence feed—even though the vendor may package these threat feeds into one annual subscription.

Licensing threat intelligence feeds from multiple vendors for a single product adds complexity from both a product development and legal (i.e., contractual) standpoint. This increases product development and back office (e.g., legal, accounting) costs. Security vendors with broad product portfolios—such as web security, email security, endpoint security, and/or mobile security products—exacerbate the problem, as they typically require every category of threat intelligence under the sun!

INFREQUENT INTELLIGENCE UPDATES

The frequency of threat intelligence updates varies by category. Some threat feeds should be updated daily (e.g., web classification, mobile app reputation) while others should be updated continuously throughout the day (e.g., web reputation, IP reputation, anti-phishing, file reputation, mobile security). Unfortunately, threat intelligence sourced from smaller vendors and open source projects often fall short of leading threat intelligence vendors as they simply don't have the infrastructure or manpower to update their feeds at such rigorous intervals.

PROPENSITY FOR FALSE POSITIVES AND FALSE NEGATIVES

We live in the real world. Not everything you perceive is 'right' or 'wrong.' The same holds true for classifying cyberthreats. Some threats are obviously bad while others aren't threats at all. Unfortunately, there are many potential threats that live in between. Your automated analysis processes may assign a web reputation score of 50 (on a scale of 1 to 100), for example, meaning that a particular URL is suspected of being malicious, but there isn't enough evidence to prove it.

When there are too many potential threats that are neither classified as 'known good' nor 'known bad,' the greater the potential for false positives (i.e., good traffic misclassified as bad) and false negatives (i.e., bad traffic misclassified as good.). The former is an inconvenience while the latter can be a company killer.

Unfortunately, low- and no-cost threat intelligence providers typically lack the ability to accurately score potential threats as they don't have the means to correlate potential threats across disparate threat feeds to 'build a case' for more accurate threat classification.

LIMITED GEOGRAPHIC PRESENCE

Threats vary by geography. It's as simple as that. Multi-national enterprises simply can't afford to acquire a security product with threat intelligence that is derived from the United States alone. The problem is that most threat intelligence vendors and open source projects emanate from the United States. Unfortunately, low- and no-cost providers are often limited in their ability to capture raw threat intelligence on a global basis.

JUGGLING MULTIPLE DEVELOPER APIs

Another challenge with sourcing threat intelligence that affects the software developers is juggling multiple APIs for different threat feeds. If you obtain threat intelligence from six vendors and/or open source projects, you'll find that each provider has its own API with different integration methodologies for each. This increases software development costs and complexity.

THREAT INTELLIGENCE OEM PARTNER SELECTION CRITERIA

Now that you have a handle on the challenges security vendors commonly face when evaluating threat intelligence providers, let's now explore key criteria for selecting (hopefully just one) an OEM partner.

CRITERION #1: COMPREHENSIVE SERVICE OFFERINGS

Partnering with multiple threat intelligence OEM partners can be challenging from legal, accounting, and product development perspectives. Ideally, all of your threat intelligence licensing agreements should 'co-term' so they begin and end all at the same time—which is challenging when you source various threat feeds from multiple providers.

To overcome these challenges, don't give up on the notion of sourcing all necessary threat intelligence feeds from a single OEM partner. Even if you can narrow the list down to two or three providers, you'll save yourself lots of headaches in the long run.

CRITERION #2: 'BIG DATA' APPROACH

Establishing and maintaining a cloud-based global threat intelligence infrastructure is a monumental—and very expensive—effort. If done well, your customers' networks will be well defended. If done poorly, your customers may make headlines for all of the wrong reasons and you may be out of a job.

Aggregating millions of domain names, IP addresses, and mobile apps and billions of URLs and file behavior records requires a 'Big Data' approach called 'maximum entropy discrimination' (MED). MED is the evolution of first-generation 'Bayesian networks' and second-generation 'support vector machines' (SVM) techniques used to prioritize feeds for human analysis. MED uses advanced algorithms and machine learning to perform automated cloud-based analysis of threats in massive volumes with remarkable speed and accuracy.

Most smaller providers update their threat intelligence feeds less frequently not because they're lazy, but because they simply don't have enough updated threat intelligence to share. This is typically not a problem with larger, more established providers that feature a Big Data approach to threat intelligence aggregation.

CRITERION #3: INTELLIGENCE CORRELATION

Even if you select a single vendor for all of your threat intelligence needs, and even if that vendor has adopted a MED-based Big Data approach, that doesn't mean they're any more likely to reduce false positives or false negatives. Remember, not all threats are black and white. Some potential threats are much harder to classify as good or bad.

In an effort to reduce false positives and false negatives, leading threat intelligence providers have developed correlation techniques that automatically cross reference web reputation feeds against IP reputation, file threat intelligence, and other intelligence sources to add contextual awareness and help reduce the quantity of uncategorized potential threats. For example, when a previously unclassified URL is later linked to a malware-infected file or perhaps a known-bad IP address, that URL is now much easier to classify as known bad.

When evaluating threat intelligence OEM providers, be sure to ask if—and, if applicable, how—the vendor is able to correlate threats from multiple feeds in an effort to reduce false positives and false negatives. If they lack this capability, it's in your best interest to locate a vendor that can.

CRITERION #4: BROAD GEOGRAPHIC REACH

As mentioned earlier, cyberthreats vary by geographic region. If your customers operate globally, then it's critically important that threat intelligence aggregated by your OEM partner emanates from aggregation points in countries where your customers do business. Otherwise, your U.S.-based customers may be well protected, but your international customers may not be.

CRITERION #5: EASE OF INTEGRATION

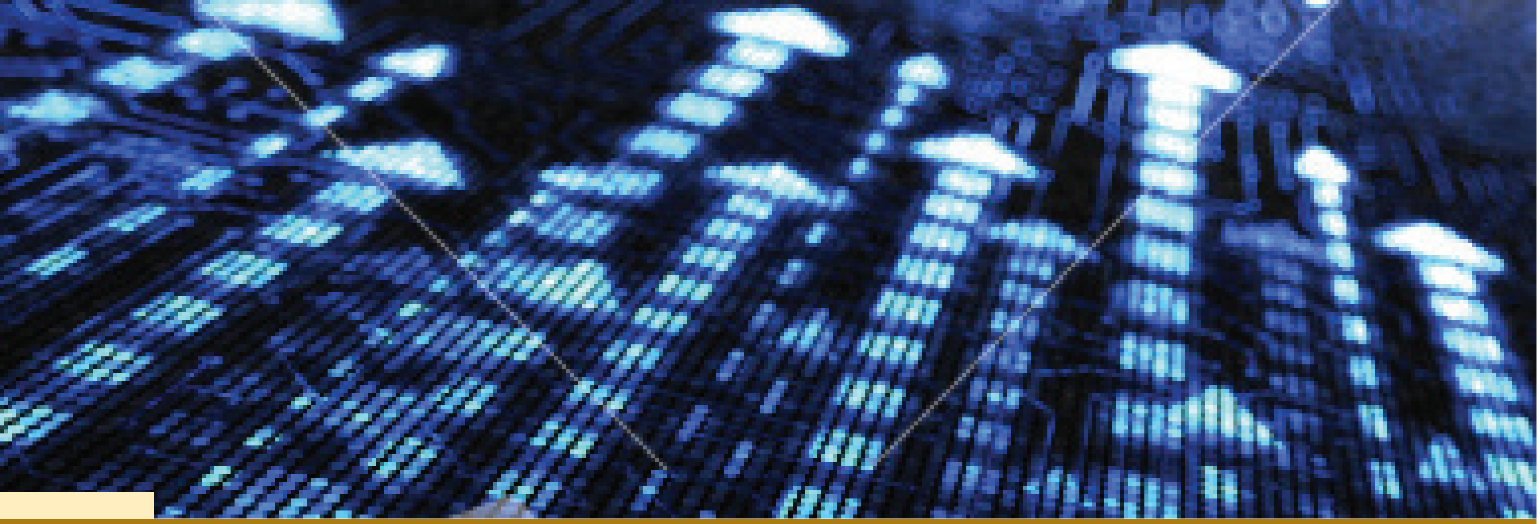
Selecting one OEM partner for all of your threat intelligence needs certainly makes life simpler. But so does using one API for all of your licensed threat intelligence feeds. If your chosen vendor provides a different API for each of its threat intelligence feeds, then this partly defeats the purpose of seeking one OEM partner.

Do your best to locate one threat intelligence OEM partner with one API for all of its threat feeds. Your developers will thank you.

CONCLUSION

When it comes to cyberthreats, the only constant is change. Threat actors change, targets change, and the methods used to deliver threats are constantly evolving. Having comprehensive and highly accurate threat intelligence is critical to the success of any security product designed to mitigate threats. Unfortunately, locating an ideal threat intelligence OEM partner is not a trivial task. No two providers are the same. The quality and quantity of threat data varies widely by provider.

The challenges you'll face when evaluating threat intelligence providers are numerous and compelling. Take the time to apply the five aforementioned selection criteria when evaluating potential OEM partners for Internet, file, and/or mobile threat intelligence. Selecting the right partner is a crucial decision that can make or break your company—and potentially your customers' companies, as well.



About Webroot

Webroot is the market leader in cloud delivered security software as a service (SaaS) solutions for consumers, businesses and enterprises. We have revolutionized Internet security to protect all the ways you connect online. Webroot delivers real-time advanced internet threat protection to customers through its BrightCloud security intelligence platform, and its SecureAnywhere suite of security products for endpoints, mobile devices and corporate networks. Over 7 million consumers, 1.5 million business users and 1.3 million mobile users are protected by Webroot. Market leading security companies, including Cisco, F5, gateprotect, Palo Alto Networks, RSA, SOTI, Telenor, and others choose Webroot to provide advanced Internet threat protection for their products and services. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held internet security company in the United States – operating globally across North America, Europe and the Asia Pacific region. For more information on our products and services, visit www.webroot.com.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles. For information, connect to our website at www.cyber-edge.com.

CYBEREDGE GROUP

CyberEdge Group, LLC
1997 Annapolis Exhange Pkwy
Suite 300
Annapolis, MD 21401

800.327.8711
info@cyber-edge.com
www.cyber-edge.com

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of CyberEdge Group, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.

Copyright © 2014, CyberEdge Group, LLC. All rights reserved. The CyberEdge Group logo is a trademark of CyberEdge Group, LLC in the United States and other countries. All other trademarks are the property of their respective owners.