A CyberEdge Group White Paper

September 2017

Tactical Threat Intelligence: The Foundation for Five OEM Use Cases

Sponsored by:

WEBROOT®

CYBEREDGE GROUP

INTRODUCTION

Cyber threats are increasingly effective at infiltrating networks and causing serious harm. Sophisticated solutions help your customers prevent intrusions and deflect dangerous communications, but they must be armed with tactical threat intelligence to accurately distinguish benign traffic from malicious.

> "Today's threats call for dynamic, next-generation threat intelligence."

Not all threat intelligence is created equal. With no generally accepted benchmarks, vendor offerings vary widely. Some are static lists that are updated infrequently, while others are timelier, but not subject to rigorous analysis that would ensure accuracy. Today's threats call for dynamic, next-generation threat intelligence. This means technical indicator feeds that provide broad coverage, including domains, IP addresses, and hashes. The feeds need to be updated constantly because a website that posed no threat yesterday could be highly malicious today. They must be accurate, since false positives or negatives could impact your customers' security and productivity. They should span a large geographic area to cover a global customer base, and they must be easy to integrate into your offerings. By incorporating next-generation tactical threat intelligence, you can help your customers improve their security posture and avoid harmful breaches. It's all about quality, timeliness, accuracy and delivery.

> "It's all about quality, timeliness, accuracy and delivery."

While threat intelligence is a key ingredient in many solutions, the specific requirements differ in terms of content, context, quality, speed and support. To better understand the differences, and how to choose the best tactical threat intelligence solution for your offering, this paper discusses five use cases. Each is presented in terms of the problem to be solved and the ultimate goal, complicating factors, and the basic requirements for threat feeds. These use cases—for Application Delivery Controllers (ADC) solutions, next-gen firewalls, IPSs, gateways and wireless access points—serve as a roadmap to quickly achieve your goals while avoiding some common pitfalls. The threat intelligence solutions we will be highlighting and recommending include:

- IP Reputation
- Web Classification
- Web Reputation
- Real-Time Anti-Phishing
- File Reputation

USE CASE 1: ENHANCING ADC SOLUTIONS WITH IP REPUTATION SERVICES

Application delivery controllers (ADCs) are designed to improve the performance, security, and resiliency of applications delivered over the internet. ADC vendors incorporate IP reputation service feeds to detect and block malicious activity before it hits the network. Accuracy and timeliness are especially important.

PROBLEM

ADCs serve as a natural entry point into the network, for good traffic as well as bad. As cyber attacks increase, ADCs are subject to growing threats coming from rapidly changing IP addresses, as well as inbound and outbound botnet traffic, such as DDoS attacks and malware activity. In order to detect and block malicious activity before it hits the data center (and increases in processing demands), ADCs need full visibility into the context of inbound connections.

CHALLENGES

It would be relatively straightforward for ADCs to detect malicious traffic if it came from a known set of IPs with bad reputations. But IPs change, as do reputations. In fact, more than 100,000 previously benign websites are reclassified as malicious every day[1]. Periodically updated threat feeds are not good enough; they can't include the most recently compromised IPs or remove newly benign ones.

Creating further complications, many threat feeds only cover a narrow geographic area and have few input sources. They don't include detailed contextual information on malicious IPs, so incident response teams have a hard time investigating threats quickly. And many are difficult to incorporate into the ADC solution. Real-time, dynamic, global IP threat intelligence is the only way to keep up with relentlessly changing IPs, reducing risk while improving data center efficiency.

REQUIREMENTS/SELECTION CRITERIA

Choosing the right tactical threat intelligence service for ADCs means making sure the solution can demonstrably meet or exceed the basic requirements to satisfy your customers' needs.

Coverage: The solution should provide coverage and visibility through a wide range of high-quality input sources. It should be based on a global threat sensor network, and the threat intelligence database should include tens of millions of IPs at any given time.

Context: The solution should provide reputation intelligence to correlate IP data with URL, file, and mobile applications, alert on suspicious activities, and provide detailed contextual information on each malicious IP found.

Timeliness: The threat intelligence database should be updated as often as every five minutes, in addition to full daily updates that include net new IPs. This lets you correlate traffic with highly accurate, real-time IP reputation data.

Accuracy: Because IPs are not on the black list forever, the solution should release IPs as needed. The best solution will employ a methodology for periodically reviewing IPs on the black list, releasing those that are no longer harmful. This ensures the list is fresh and updated frequently.

Delivery: The solution should be easy to deploy and integrate. Simple integration via RESTful APIs and a dynamic SDK lets you keep up with changes to the threat landscape.

WHAT TO EXPECT

Choosing the right tactical threat intelligence solution helps you differentiate yourself from your competition. By providing your customers with optimized protection against tens of millions of malicious IPs based on real-time updates, your solution is far more powerful than an ADC that uses static lists. When sold as an additional offering, it can result in increased revenue and a broader solution portfolio. Of course, the direct benefits to your customers are another layer of defense against cyber attacks, enhanced application performance and availability, and improved data center productivity.

> "Choosing the right tactical threat intelligence solution helps you differentiate yourself from your competition."

USE CASE 2: EXTENDING NEXT-GEN FIREWALLS WITH WEB CLASSIFICATION AND REPUTATION

Next-generation firewalls (NGFWs) detect and block sophisticated attacks by enforcing security policies at the application level, as well as at the port and protocol level. NGFW vendors incorporate web classification and reputation feeds to gain complete visibility and control over the traffic that traverses the edge device.

PROBLEM

By themselves, NGFWs are unable to differentiate a benign IP from a malicious IP without some source of intelligence. It's especially difficult to get complete visibility and control at Layer 7, where most cyber attacks take place. Most NGFWs employ static lists of malicious IPs and URLs that are loaded in at boot time. Because IPs change frequently, these lists are out of date as soon as they are published. And because most lists only look at the most popular sites, they miss new URLs and infrequently visited sites, leading to inaccurate results. Without the right threat intelligence, the firewall can't prevent your customers' users from accessing malicious or inappropriate websites.

CHALLENGES

Network performance is critical, so requests must be serviced quickly. However, a firewall can easily flood the network security team with too many alerts and false positives, hampering their ability to understand and respond to new threats. Perhaps a bigger complication is that many NGFW devices can consume only a limited amount of data due to memory, disk, and CPU limitations.

REQUIREMENTS/SELECTION CRITERIA

NGFW vendors looking for tactical threat intelligence solutions will demand a close match to their unique requirements for accuracy, timeliness, speed, performance and ease of integration.

Coverage: Going beyond the normal lists of popular sites, the optimal solution should provide extensive coverage of domains (more than 600 million) and URLs (more than 27 billion). To provide such extensive coverage, it should include "long tail" classifications: new URLs, as well as those that do not have many visits and thus are ranked low on public searches. Such sites could be malicious or phishing sites, or could pose compliance issues.

Timeliness: The solution should guarantee very frequent database updates—multiple times per hour—to ensure that IP reputations are current. To do this, the vendor must have registered with all zone lists, and scan through classifiers as soon as a domain name is registered.

Accuracy: Make sure the solution utilizes advanced machine learning algorithms coupled with analysis by human experts, to classify internet objects at blazing speed with high accuracy. Look for a provider who can analyze uncategorized sites at a rate of around 5,000 URLs per second. This is the only way to stay ahead of evolving threats.

Performance: A combination of a local SDK and a cloud service provides the performance that today's networks require. The service should deliver intel via a direct ingest or a direct API call to a predictive threat intelligence service. Make sure the vendor can guarantee sufficient performance -we suggest 50-100 requests per second at the local SDK level, and 20K requests per second per server from the cloud service – to ensure continuously updated risk scores. If the service can tailor results to what's relevant to the organization (as opposed to the entire internet) this helps performance as well.

Delivery: NGFW providers look for solutions that are easy to deploy and integrate via SDKs and APIs.

WHAT TO EXPECT

NGFW providers can offer enhanced safety to their customers, giving them the ability to truly control how their users access the web. This means unprecedented protection against a full spectrum of legal, regulatory, productivity and compliance issues. Done right, the solution can enhance productivity and resource utilization with quick time-to-value through easy integration. It can be provided as an upsell security subscription service, leading to incremental revenue.

"This means unprecedented protection against a full spectrum of legal, regulatory, productivity and compliance issues."

USE CASE 3: EXPANDING THE SCOPE OF INTRUSION PREVENTION SYSTEMS WITH THREAT INTELLIGENCE

Intrusion prevention systems (IPSs) actively analyze and take automated actions on all traffic flows that enter the network to detect and prevent exploits. IPS vendors need to incorporate actionable threat intelligence on spam, phishing, botnets, malicious websites and the like, to differentiate their offering and provide a complete solution.

PROBLEM

Legacy IPSs identified and blocked attack traffic at the gateway, based on signatures. Not only was this approach compute-intensive, it was also ineffective, as attackers found ways to evade signature-based tools. Newer IPSs block all connection attempts from specific IP addresses or domains, relying on static lists of known bad IPs. This problem is obtaining reputation feeds that are updated frequently enough to reflect the true current state of IPs.

CHALLENGES

IP reputation is fluid. An IP associated with phishing or ransomware today could be benign tomorrow. Inaccurate information can be devastating, since a false positive can result in frustrated users while a false negative can lead to a breach. The information must be updated continually, with fast, reliable performance. As an inline security service, the IPS must work efficiently to avoid degrading network performance, and must be fast enough to avoid near-real-time exploits.

REQUIREMENTS/SELECTION CRITERIA

IPS vendors should evaluate tactical threat intelligence solutions based on coverage, frequency of update, performance, accuracy and delivery.

Coverage: The best solution will provide coverage of more than 600 million domains and billions of URLs. It will avoid the common limitation of only focusing on popular sites; instead, it will include "long tail" classifications: new URLs, as well as those that do not have many visits and thus are ranked low on public searches. Such sites could be malicious or phishing sites, or could pose compliance issues.

Frequency of Update: The solution should guarantee very frequent database updates—as often as every five minutes—to ensure that IP reputations are current. Ensure that the vendor has registered with all zone lists, and scans through classifiers as soon as a domain name is registered.

"The solution should guarantee very frequent database updates—as often as every five minutes—to ensure that IP reputations are current."

Performance: The service should deliver intel via a direct ingest or a direct API call to a predictive threat intelligence service. Look for performance levels of 50-100 requests per second at the local SDK level, and 20K requests per second per server from the cloud service. This will ensure that risk scores are continuously updated. And if the service can tailor results to what's relevant to the organization (as opposed to the entire internet) this will help with performance as well.

Accuracy: The best solutions will utilize advanced machine learning algorithms, augmented by human expert analysis to further boost accuracy. Look for a provider who can analyze uncategorized sites at a rate of around 5,000 URLs per second to provide accuracy at speed.

Delivery: The solution must be easy to deploy and integrate via SDKs and APIs.

WHAT TO EXPECT

IPS providers can differentiate their offerings, providing broader coverage and more protection against a spectrum of legal, regulatory, productivity and resource utilization risks than their competitors. When the right threat intelligence solution is chosen, it can be an integrated service, leading to incremental revenue and increased customer satisfaction.

USE CASE 4: BOOSTING WEB FILTERING GATEWAYS WITH WEB CLASSIFICATION/REPUTATION AND IP REPUTATION

Gateways combine multiple security services into a single platform, to provide protection via outbound web filtering for businesses of all sizes. Accurate, timely web classification and reputation and IP reputation feeds improve security.

PROBLEM

Vendors need to provide end users with the ability to apply policy to and across their gateways. Whether organization-specific constraints or broad-based regulations such, as the Internet Watch Foundation (IWF) child abuse content list, gateways need information on websites deemed malicious or undesirable. The normal approach is to take a series of static lists of known bad URLs and IPs and join them together to create a more complete list in hopes of blocking malicious websites.

CHALLENGES

IPs change, as do reputations. Webroot research shows that more than 100,000 websites previously benign must be reclassified to malicious each day. This means that gateways must constantly update IPs and web addresses via threat intelligence feeds. Lists are hard to cobble together and are out of date as soon as they are produced. Inaccuracy stems from two facts: they won't include newly malicious URLs and IPs, and they probably still contain previously malicious IPs that are now benign.

In addition to accuracy issues, gateways must support the high levels of performance demanded by today's bandwidth-intensive networks. Instead of downloading and maintaining URL block lists, they need real-time, dynamic web classification/reputation and IP reputation services to provide the desired protection.

"...gateways must support the high levels of performance demanded by today's bandwidth-intensive networks."

REQUIREMENTS/SELECTION CRITERIA

Gateway vendors need to choose a tactical threat intelligence solution that provides the coverage, performance, accuracy, integration and support that will enable them to differentiate their offering and drive incremental revenue.

Coverage: Comprehensive coverage will involve hundreds of millions of domains and billions of URLs. While many tactical feeds incorporate frequently visited sites, the optimal solution will also include "long tail" classifications, encompassing both new URLs and infrequently visited but potentially malicious ones.

Performance: For devices that are memory-limited or resource-constrained, the solution should provide an option of local determination in cache, as opposed to downloading the entire database or always doing cloud-based lookups. The "smart caching" strategy enables partners to cache URLs based on their reputation score or web classification category, improving performance.

Accuracy: The best solution will scan through classifiers as soon as a domain name is registered, utilizing advanced machine learning algorithms coupled with analysis by human experts to classify objects with high accuracy. The database is updated multiple times per hour to ensure that reputations are current.

Integration and Support: The solution should be easy to deploy and integrate via SDKs and APIs. Look for a vendor that can provide education on the nature of the data being provided, as well as assistance in configuring and integrating the service as part of the solution rather than a separate, for-cost item.

WHAT TO EXPECT

Gateway vendors can ensure optimal performance with extensive coverage to fit a variety of customer sizes and use cases. Dynamic data provides both accuracy and timeliness. Because gateways provide many security services, customers benefit from enhanced protection not only from gateway web filtering but also from enhanced firewall and IPS capabilities discussed above. Finally, with the right vendor support during implementation and integration, and robust SDKs, you enjoy quick time-to-value.

USE CASE 5: SECURING WIRELESS ACCESS POINTS WITH WEB CLASSIFICATION/REPUTATION AND IP REPUTATION

Wireless access points (WAPs) allow WiFi devices to connect to wired networks. WAP vendors incorporate web classification and web/IP reputation services for content filtering to detect and block malicious activity before it hits the network. In a crowded market, web classification/reputation can help vendors differentiate their offerings while providing enhanced security to their customers.

PROBLEM

Content filtering is a delicate balance between protecting users from risks while ensuring maximum accessibility. Many content filters are based on a static list of known URLs, which are out of date as soon as they are created, and lack the granularity required for different organizational needs. With hundreds of new web sites created each minute, static lists cannot hope to provide up-to-date, accurate information. Yet extreme accuracy is exactly what is needed when identifying, classifying and blocking malicious URLs and IPs.

> "With hundreds of new web sites created each minute, static lists cannot hope to provide up-to-date, accurate information.

CHALLENGES

Some threat intelligence solutions can impact performance. When a user requests a URL, the determination must be made in real time. But some solutions require downloading a database to do local lookups—clearly impractical for resource-constrained devices. Instead, they need real-time, dynamic web classification/reputation and IP reputation services to ensure quick yet accurate results without performance implications. One further complication is the difficulty of integrating some threat intelligence feeds into WAPs.

REQUIREMENTS/SELECTION CRITERIA

WAP vendors want to choose a web classification/reputation solution with the accuracy and coverage they need, but with a strong emphasis on performance and support to ensure quick time-to-value and strong product differentiation.

Accuracy and Coverage: Comprehensive coverage will involve hundreds of millions of domains and billions of URLs, while accuracy comes from the use of advanced machine learning algorithms coupled with analysis by human experts. The optimal solution will cover not just those sites that are visited frequently, but also include "long tail" classifications: new URLs and infrequently visited sites that could be malicious. With real-time updates, partners can ensure their customers are always receiving the most up-to-date, accurate results.

Performance: WAPs are small, memory-limited devices that cannot download a full database. Choose a solution that only caches what the customer has looked up: local determinations in cache, as opposed to

cloud-based lookups or calls can increase the speed and performance of the WAP. This "smart caching" strategy enables partners to cache URLs based on their reputation score or web classification category. With a small initial footprint, the cache can grow over time as needed.

Integration and Support: The solution should be easy to deploy and integrate via SDKs and APIs. Look for a vendor who can provide education on the nature of the data being provided, as well as assistance in configuring and integrating the service as part of the solution rather than a separate, for-cost item.

WHAT TO EXPECT

WAP vendors can differentiate their offerings from competitors by providing additional security without impacting performance. Broad coverage of domains and URLs provides an easy fit with customers' unique requirements. Accurate and timely web classification and reputation enables protection from internet-related risks at near real-time speeds, while smart caching avoids performance problems. And technical assistance during the SDK-based integration means quick time-to-market for a truly differentiated offering.

CONCLUSION

Every use case calls for a specific mix of capabilities to meet somewhat different requirements. However, there are common threads that run throughout any partner's architecture list for tactical threat intelligence.

Accuracy is of the utmost importance for any use case. The service should provide broad coverage of new and infrequently visited sites, as well as popular sites, so that nothing is missed. The service should also employ machine learning algorithms, coupled with human expert review, so that the results are highly accurate.

Timeliness is key. Requests must be serviced at real-time or near-real-time speed, which means the threat intelligence database must be kept up to date constantly. When updates happen as often as every five minutes, the time to identify IP threats is drastically reduced.

Update Frequency can't be stressed enough. Because IPs are not on the block list forever, the right solution incorporates a methodology for periodic review and release of no-longer-harmful IPs. This ensures the database is fresh and is updated frequently enough to guarantee accuracy and timeliness.

Not all threat intelligence is created equal. Use the recommended selection criteria as a guideline for choosing the best solution for your unique needs. Differentiate your offering from the competition with industry-leading protection against millions of malicious IPs and unwanted content. Harness the collective intelligence from millions of sources via the world's most powerful cloud-based security network. Integrate quickly and easily into your solution for quick time-to-market and incremental revenue.

> "Not all threat intelligence is created equal."

For more information and guidance on incorporating accurate, timely, up-to-date threat intelligence into your solutions and services, visit www.webroot.com/brightcloud.

Footnotes:

1. Webroot 2016 Threat Brief, February 2016

About Webroot

Webroot delivers next-generation endpoint security, network security, threat intelligence services, and security awareness training to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® solution protect millions of devices across businesses, home users, and the Internet of Things. Webroot is trusted and integrated by market-leading companies, including Cisco, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at 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 more information about CyberEdge and our 50+ services, connect to our website at https://www.cyber-edge.com.

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

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